МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ МІЛІЦІЇ

НАУКОВО-ДОСЛІДНА ЛАБОРАТОРІЯ З ПРОБЛЕМ ПРОТИДІЇ ЗЛОЧИННОСТІ

ДІЯЛЬНІСТЬ ОРГАНІВ ВНУТРІШНІХ СПРАВ ЩОДО МІНІМІЗАЦІЇ ІНТЕРНЕТ-РИЗИКІВ

Науково-методичні рекомендації

Харків – 2014

Авторський колектив:

Бугайчук Костянтин Леонідович, к.ю.н., доцент, провідний науковий співробітник науково-дослідної лабораторії з проблем протидії злочинності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції Харківського національного університету внутрішніх справ.

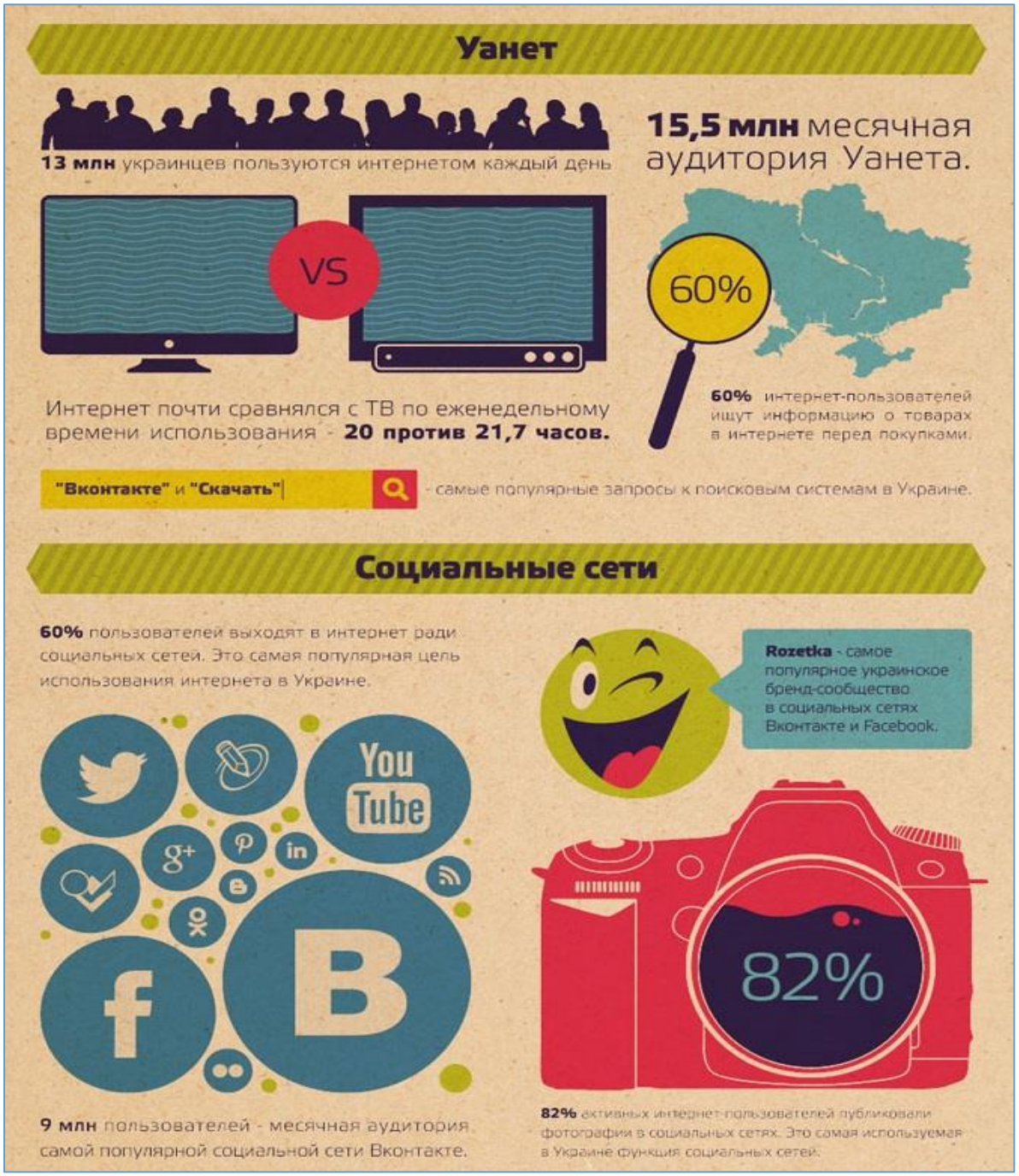
Схвалено на засіданні науково-дослідної лабораторії з проблем протидії злочинності «20» червня 2014 р., протокол № 6

Бугайчук К.Л. Діяльність органів внутрішніх справ щодо мінімізації Інтернет-ризиків [Текст] : наук.-метод. рек. / К.Л.Бугайчук. – Х. : Харк. нац. ун-т. внутр. справ. – 2014. − 72 с.

ЗМІСТ

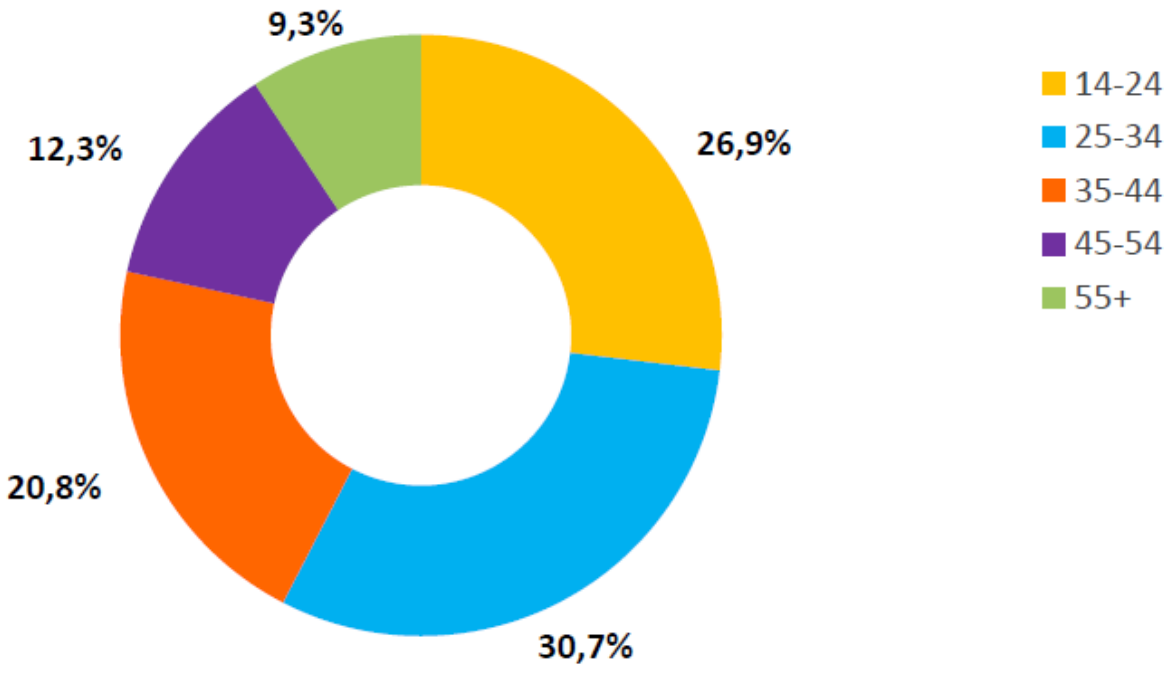
1.1. АКТУАЛЬНІСТЬ ПИТАННЯ: ЯК УКРАЇНЦІ КОРИСТУЮТЬСЯ ІНТЕРНЕТ?

Інформатизація сучасного українського суспільства зробила всесвітню мережу Інтернет елементом життя кожного українця. Як і будь-яке соціальне явище користування Інтернет пов'язано як з позитивними, так і негативними аспектами. Для їх повного розуміння багато соціологічних та маркетингових компаній проводять дослідження Інтернет аудиторії на Україні.[1]

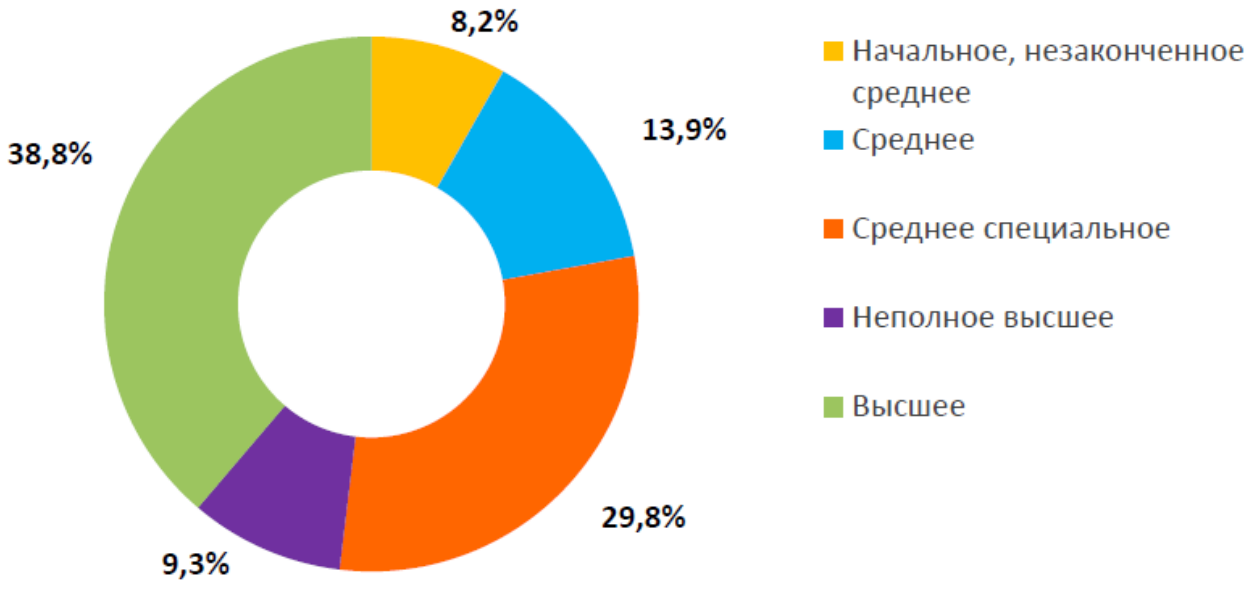


1 Аудиторія Уанета за березень 2014 року: Дослідження gemiusAudience. – В звіті представлені 522 сайта. Соціально-демографічний звіт складений на підставі 44 262 анкет и 6 754 софтверних панелистів. – Режим доступу: www.gemius.com.ua (contact@gemius.com.ua)

СОСТАВ АУДИТОРИИ ПО ВОЗРАСТУ



СОСТАВ АУДИТОРИИ ПО ОБРАЗОВАНИЮ



Окрім соціально-демографічних характеристик, досліджуються уподобання Українців в Інтернет.[2] На кінець 2013 року 50% українців віком старше 16 років регулярно користувались Інтернетом, найпопулярнішими причинами користування серед українців залишаються соціальні мережі. Кожен другий українець віком 16 років і старше користувався Інтернетом принаймні один раз на місяць. Цей показник зріс у порівнянні з показником за аналогічний період 2012 року. Найактивніші користувачі мережі – це, звичайно, молодь. Так, серед вікової групи 16-19 років 70% українців щоденно заходять в Інтернет, тоді як у віковій групі 50-59 років таких лише 14%. Чоловіки та жінки користуються соціальними мережами і електронною поштою на одному рівні. Поряд з цим є ряд причин з яких чоловіки частіше заходять в мережу, ніж жінки, а саме: завантаження музики та фільмів (48% чоловіків проти 39% жінок), перегляд телепрограм, онлайн-відео та прослуховування радіостанцій (34% проти 27%), гра в комп'ютерні ігри (30% проти 16%). Інформацію про здоров'я, навпаки, частіше шукають жінки, ніж чоловіки – 32% проти 19%.

Дослідження компаній, що займаються проблемами безпечного Інтернету показують, що, наприклад, 89,1% користувачів Інтернет бояться, що можуть стати жертвами кіберзлочинності. Такі дані міжнародного дослідження, яке провела компанія ESET. Переважна більшість Інтернет-користувачів вважає, що до будь-якими даними, які знаходяться в мережі, можуть отримати доступ

[2] GfK Ukraine: Регулярне дослідження ринку телекомунікаційних послуг серед населення України віком 16 років і старше (станом на 01.01.2014). – Режим доступу: www.gfk.ua (Solomiya.Hlibovytska@gfk.com)

сторонні особи. Це означає, що рівень довіри рядових користувачів до онлайн-сервісів, на яких зберігається їх інформація, є дуже низьким. 70,9% респондентів визнають особисту відповідальність за збереження персональної інформації, яку вони пересилають електронною поштою, розміщують в різних сервісах, соцмережах і т. ін.[3]

5 травня 2014 року компанія «Київстар» у партнерстві з Чернігівським національним педагогічним університетом імені Т. Г. Шевченко реалізувала проект «Безпечний Інтернет від «Київстар»» в рамках соціальної програми оператора «Безпека дітей в Інтернеті». За сприяння компанії «Київстар» у квітні цього року студенти Чернігівського педагогічного університету провели соціальне опитування на тему «Моніторинг загроз і ризиків безпеки дитячої та підліткової Інтернет-аудиторії», в якому взяли участь 1004 учня 6-7 класів шкіл № 1, 9, 12 , 20, 22, 27, 28, 29, 30, 31 у віці від 11 до 13 років. Результати опитування школярів наступні:

– 48% респондентів вважають Інтернет безпечним онлайн-простором, який не несе ніяких загроз;

– 47% опитаних дітей стають жертвами приниження в мережі, 14% з них – частіше 2 разів на місяць;

– 67% опитаних спілкуються в мережі з особами, з якими вони не знайомі в реальному житті, а 18% з них ходили на зустрічі з незнайомцями;

– 50% дітей взагалі не обговорюють з батьками те, чим вони займаються в Інтернеті.[4]

За даними всеросійського опитування «діти в Інтернеті» більше половини росіян (57%) висловлюють занепокоєння у зв'язку з тим, що «всесвітня павутина» містить великі обсяги шкідливої для дітей інформації (агресивного, еротичного змісту), від якої дитини неможливо вберегти. А 36% респондентів упевнені, що завдяки сучасним технологіям можна легко закрити доступ до небажаних Інтернет-ресурсів. Побоювання у зв'язку з беззахисністю дітей від шкідливої інформації зазвичай висловлюють люди у віці старше 60 років (61%), тоді як 18-24-річні частіше говорять про наявність засобів відповідного захисту (48%).[5]

---

[3] 89% пользователей Интернета боятся киберпреступности [електронний ресурс]. – Режим доступу: http://searchnews.info/53812-89-polzovateley-interneta-boyatsya-kiberprestupnosti.html

[4] «Київстар» навчив школярів Чернігівщини правилам онлайн-безпеки [Електронний ресурс]. Режим доступу: http://www.kyivstar.ua/ru/uz-15/press_center_new/reporters/releases/?id=43704

[5] Ініціативне всеросійське опитування Діти в Інтернеті: заохочувати або обмежувати?» [Електронний ресурс]. – Режим доступу: http://wciom.ru/index.php?id=459&uid=114772 (проведено 29-30 березня 2014 Опитано 1600 чоловік в 130 населених пунктах в 42 областях, краях і республіках Росії. Статистична похибка не перевищує 3,4%.)

Отже, можна констатувати, що сьогодні кількість користувачів мережі Інтернет постійно зростає, причому частка молоді та зовсім юної аудиторії серед користувачів дуже велика. Для багатьох, особливо молодих людей, Інтернет стає інформаційним середовищем, без якого вони не уявляють собі життя. Але, вміщаючи в себе великий інформаційний, навчальний та розважальний потенціал, Інтернет може бути небезпечним та становити певний ризик.

Крім того, спостерігається небезпека щодо захисту персональних даних в Інтернет при здійсненні банківських операцій, Інтернет-покупок, спілкуванні у соціальних мережах, тощо – так і суспільні явища мають узагальнюючу назву **«Інтернет-ризики».** Органи внутрішніх справ, як суб'єкт забезпечення прав і свобод громадян повинен здійснювати планомірну попереджувальну роботу в цій сфері та виробити адекватні заходи протидії таким явищам

Зважаючи на це, можна зробити висновок про актуальність пропонованої тематики.

1.2. КЛАСИФІКАЦІЯ ІНТЕРНЕТ-РИЗИКІВ[6]

1.2.1. Контентні ризики

Контентні ризики – це матеріали (тексти, зображення, аудіо, відеофайли, посилання на сторонні ресурси), що містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.ін. Зіткнутися з ними можна практично скрізь: це і сайти, і соціальні мережі, і блоги, і торренти, і відеохостінги, фактично все, що зараз існує в Інтернеті. Найчастіше подібний матеріал може прийти від незнайомця поштою у вигляді спаму або повідомлення.

Негативний контент матеріали можна умовно розділити на:

– *незаконний,* до якого можуть належати: дитяча порнографія (включаючи виготовлення, поширення і зберігання); наркотичні засоби (виготовлення, продаж, пропаганда вживання), всі матеріали, що мають відношення до расової чи релігійної ненависті (екстремізм, тероризм,

[6] В основі дослідження лежить розроблена Фондом Розвитку Інтернет та Фондом «Діти онлайн» класифікація Інтернет – ризиків: - Режим доступу: http://www.saferinternet.ru http://detionline.com/helpline/risks

націоналізм), а також ненависті або агресивної поведінки по відношенню до групи людей, окремої особистості або тварин), азартні ігри і т. ін.

Внутрішнє законодавство України передбачає різні види покарання за поширення такої інформації, про що мова піде нижче.

– неетичні, що суперечать прийнятим у суспільстві нормам моралі і соціальним нормам.

Подібні матеріали не потрапляють під дію Кримінального кодексу України, однак можуть чинити негативний вплив на психіку людини, що зіткнулися з ними, особливо дитини. Прикладами таких матеріалів можуть служити широко поширені в мережі зображення сексуального характеру, агресивні онлайн ігри, азартні ігри, пропаганда нездорового способу життя (вживання алкоголю, тютюну, анорексії[7], булімії[8]), принесення шкоди здоров'ю і життю (різні способи самогубства, курильні суміші), нецензурна лайка, образи, та ін. Інформація, що відноситься до категорії неетичної може бути також спрямована на маніпулювання свідомістю і діями різних груп людей.

Контентні ризики пов'язані з іншими типами ризиків мережі Інтернет. Наприклад, перегляд тих чи інших відео-матеріалів може призвести до зараження комп'ютера вірусами і втрати важливих даних. Дуже багато розповсюджувачів подібного негативного контенту переслідують мету заразити комп’ютер, щоб надалі мати можливість маніпулювати даними і діями зараженого комп'ютера. Пропаганда негативних матеріалів також може йти через соціальні мережі, блоги, різні форуми. У даному випадку контентні ризики перетинаються з комунікаційними.

1.2.2. Комунікаційні ризики

Комунікаційні ризики пов'язані з міжособистісними відносинами Інтернет-користувачів і включають в себе ризик піддатися образам і нападкам з боку

---

[7] **Анорéксія** (від грецького ανορεξία = без апетиту) — захворювання, що характеризується критичним зниженням маси тіла, часто небезпечним для життя, втратою апетиту. Анорексія часто виникає на нервовому ґрунті, особливо у дівчат і молодих жінок, одержимих бажанням схуднути. Анорексію часто супроводжує підвищене почуття голоду – булімія.

[8] **Нервова булімія** (від грец. βοῦς - бик і λῑμός - голод) - розлад прийому їжі, що характеризується різким посиленням апетиту, наступаючим зазвичай у вигляді нападу і супроводжується відчуттям болісного голоду, загальною слабкістю. Пацієнти, що страждають булімією, також часто вдаються до активного контролю ваги за допомогою викликання блювоти або використання проносних засобів, проте це не є симптомом захворювання. Надмірна їжа і примусове очищення шлунку в поєднанні зі слабкістю нервової системи можуть привести до серйозних ускладнень: від неврастенії, руйнування взаємин з близькими і втрати інтересу до життя до лікарської або наркотичної залежності і смерті.

інших. Прикладами таких ризиків можуть бути: незаконні контакти (наприклад, грумінг), кіберпереслідування, кібербулінг та ін Для подібних цілей використовуються різні чати, онлайн-месенджери (ICQ, Google Hangouts, Skype та ін), соціальні мережі, сайти знайомств, форуми, блоги і т.ін.

Навіть якщо більшість користувачів існуючих чат-систем мають добрі наміри, існує, на жаль, зростаюче число людей, що використовують ці бесіди зі злим умислом. У деяких випадках вони хочуть обманом змусити користувачів видати особисті дані, такі як домашня адреса, телефон, паролі до персональних сторінок в Інтернеті та ін. В інших випадках, наприклад щодо дитини, вони можуть виявитися педофілами в пошуках жертви. Видаючи себе за однолітка і встановлюючи дружні стосунки з дитиною, вони вивідують про нього багато інформації і примушують до особистої зустрічі.

Опинитися жертвою набагато простіше, ніж здається. Це біда не тільки соціальних мереж. На будь-якому популярному форумі, в блоговому співтоваристві і чаті з’являються такі учасники, які хамлять і ображають інших учасників.

Комунікаційні ризики включають в себе «незаконний контакт» і «кіберпереслідування» (або кібер-буллінг).

1. Незаконний контакт – це спілкування між дорослим і дитиною, при якому дорослий намагається встановити більш близькі відносини для сексуальної експлуатації дитини. Це поняття включає в себе такі Інтернет-злочини як домагання і грумінг.

– домагання - поведінка, що порушує недоторканність приватного життя особи. Така поведінка може полягати у прямих або непрямих словесних образ або погроз, недоброзичливих зауваженнях, грубих жартах або інсинуаціях, небажаних листах або дзвінках, показі образливих або принизливих фотографій, залякуванні, хтивих жестах, непотрібних дотиках, поплескування, щипки, ударах, фізичному нападі або у інших подібних діях.

– грумінг - встановлення дружніх відносин з дитиною з метою вступу у сексуальні стосунки.

2. Кіберпереслідування (або кібербулінг) – це переслідування користувача повідомленнями, що містять образи, агресію, сексуальні домагання за допомогою різних Інтернет-сервісів. Також, кіберпереслідування може приймати такі форми, як обмін інформацією, контактами; залякування; хуліганство (Інтернет-тролінг), соціальне бойкотування. За формою кібербулінг може бути не тільки словесним образою. Це можуть бути фотографії, зображення або відео жертви, відредаговані так, щоб бути більш принизливими.

Подібний принизливий контент може виходити від однієї людини або групи людей за одним або кількома електронним контактам жертви, на

електронну скриньку або в повідомленнях онлайн-месенджерів. Поширені також випадки переслідування в соціальних мережах або на подібних їм ресурсах. При цьому, крім розсилки образливих повідомлень і вивішування принизливих матеріалів, зображень або відеозаписів, булер може також зламати профіль або сторінку жертви і організувати спам-розсилку по всіх контактах жертви.

1.2.3. Кіберризики

Електронні (кібер-) ризики – це можливість зіткнутися з розкраданням персональної інформації, ризик піддатися вірусній атаці, онлайн-шахрайству, спам-атаці, шпигунським програмам і т.і н. Шкідливе програмне забезпечення використовує широкий спектр методів для поширення і проникнення в комп'ютери, не тільки через компакт-диски або інші носії, а й через електронну пошту за допомогою спаму або викачаних з Інтернету файлів.

До шкідливих програм відносяться віруси, черв'яки і «троянські коні» – це комп'ютерні програми, які можуть завдати шкоди вашому комп'ютеру і даним, що зберігаються на ньому. Вони також можуть знижувати швидкість обміну даними з Інтернетом і навіть використовувати комп'ютер для поширення своїх копій на комп'ютери ваших друзів, родичів. Захист в соціальних мережах - це завдання, яке не так давно стало актуальним для їх користувачів.

Зокрема, тепер вірусне ПЗ (програмне забезпечення), яке розсилає спам в соціальній мережі, може бути встановлено на ваш комп'ютер з будь-якого сайту. І від вашого особи можуть регулярно розсилатися абсолютно будь-які повідомлення, позбутися яких не допоможе жодна захист самого сайту. Хоча б просто з тієї причини, що в цьому випадку буде потрібний не захист вашої сторінки, а сучасне антивірусне програмне забезпечення.

На жаль, ймовірність наштовхнутися на подібні шкідливі програми дуже велика. Крім негативного впливу на комп'ютер і мобільний пристрій, можна стати жертвою ще одного виду кібер-злочини - кібер-шахрайства. У самому широкому сенсі шахрайство – це навмисний обман або зловживання довірою з метою отримання будь-якої вигоди.

Шахрайство в мережі Інтернет (кібершахрайство) – один з видів кіберзлочиниів, метою якого є обман користувачів. Розкрадання конфіденційних даних може призвести до того, що злочинець незаконно отримує доступ і яким-небудь чином використовує особисту інформацію користувача (номери

банківських рахунків, паспортні дані, коди, паролі тощо), з метою завдати матеріальний і фінансовий збиток.

1.2.4. Споживчі ризики

Споживчі ризики – зловживання в Інтернеті правами споживача. Вони включають в себе: ризик придбання товару низької якості, контрафактної і фальсифікованої продукції, втрату коштів без придбання товару або послуги, викрадення персональної інформації з метою кібершахрайства, та ін.

Також діти, часто здійснюючи онлайн покупки, можуть розтратити значні суми своїх батьків, якщо яким-небудь способом мали або отримали до них доступ. Одним з найпоширеніших видів даного типу ризиків є шахрайство – це навмисний обман або зловживання довірою з метою отримання будь-якої вигоди.

Оскільки шахрайство в мережі Інтернет скоюється за допомогою різних технічних засобів і різноманітного кількості програм, то деякі його види можуть бути віднесені і до групи електронних ризиків, а частина до групи комунікаційних, оскільки включає в свою схему встановлення більш близького контакту з жертвою протягом якого- або часу (наприклад, за допомогою електронних листів і SMS, які можуть привести і до реальних зустрічей з шахраями).

1.3. ЗАГАЛЬНІ ПИТАННЯ ЗМІСТУ ТА МІНІМІЗАЦІЇ ДЕЯКИХ ІНТЕРНЕТ-РИЗИКІВ

1.3.1 Фішинг

Фішинг – особливий вид Інтернет-шахрайства, направлений на незаконне отримання особистих та фінансових даних користувача. Для цього зловмисниками створюється спеціальний сайт, що виглядає як, наприклад, сайт банку або сайт, що здійснює безготівкові розрахунки в мережі Інтернет.

Використовуючи дані, введені користувачем на цьому сайті (ім’я, пароль, пін-код тощо), зловмисники отримують доступ до коштів потерпілого.

Яким чином відбувається фішингова атака?

Головним завданням зловмисників є заманювання користувача на створений ними сайт. Для цього використовується декілька методів.

а) Найбільш поширеним є розсилка фішингових листів.

На електронну адресу користувача надсилається лист із запрошенням перейти на сайт банку/розрахункового сайту за вказаним у листі посиланням.

Причини, які вказуються у листі, можуть бути різними:

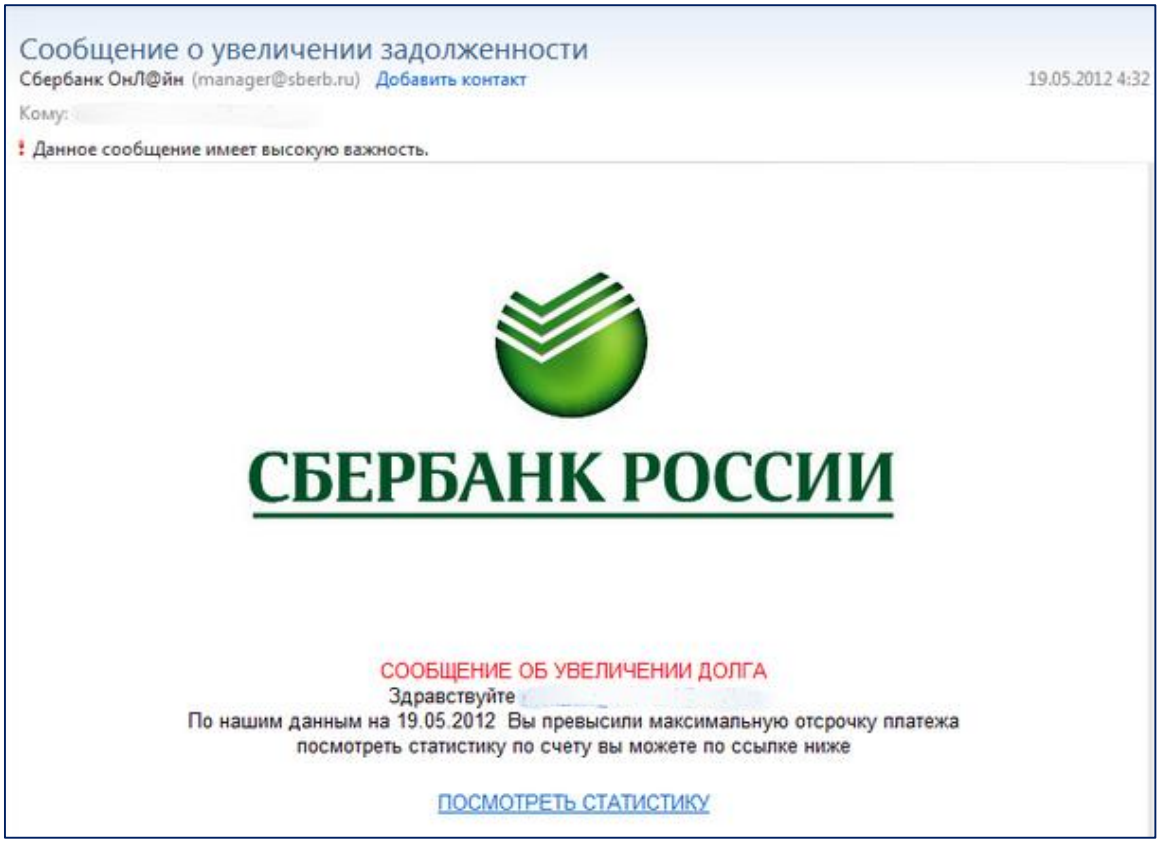
– надходження коштів на рахунок, яке необхідно підтвердити;

– проблеми з рахунком, які можливо вирішити лише перейшовши на сайт банку (інформація про збільшення заборгованості, можливе блокування рахунку тощо);

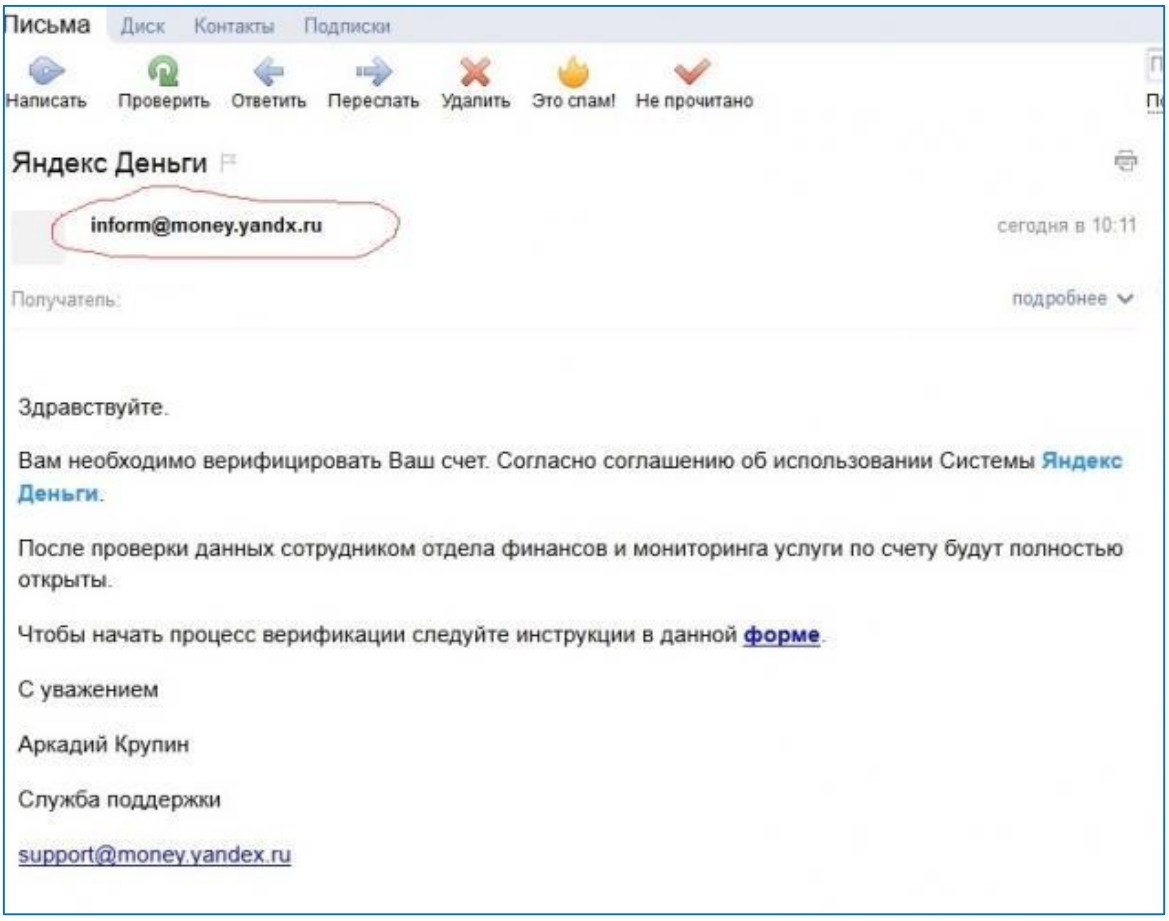
– профілактичні заходи в системі безпеки банку тощо.

При переході на створений зловмисниками сайт, потерпілому пропонують авторизуватися, увівши своє реєстраційне ім’я (логін) або номер рахунка та пароль; в окремих випадках зловмисники можуть також запропонувати ввести номер розрахункової картки та її ПІН-код.

Найчастіше фішинговий сайт виглядає як справжній. В окремих випадках підробку можна розпізнати за адресою сторінки: хоча вона зроблена таким чином, щоб нагадувати оригінальну, існують відмінності. Найчастіше це заміна окремих літер (напр. priwatbank.ua або privatbanc.ua замість privatbank.ua) або домену (напр., aval.ua.com.cn замість aval.ua) в адресі.



Фішинговий лист від банку



Фішинговий лист від платіжної системи (не співпадає адреса пошти)

Фішингові повідомлення також можуть бути у вигляді фальшивих оголошень про роботу, які можуть переконати здобувачів відправити свою особисту інформацію. Кіберзлочинці публікують свої оголошення на законних сайтах з оголошеннями про вакансії і часто використовують знайомі або переконливі логотипи компаній, мова оголошення та посилання на підроблені веб- сайти, які нібито належать реальним організаціям.

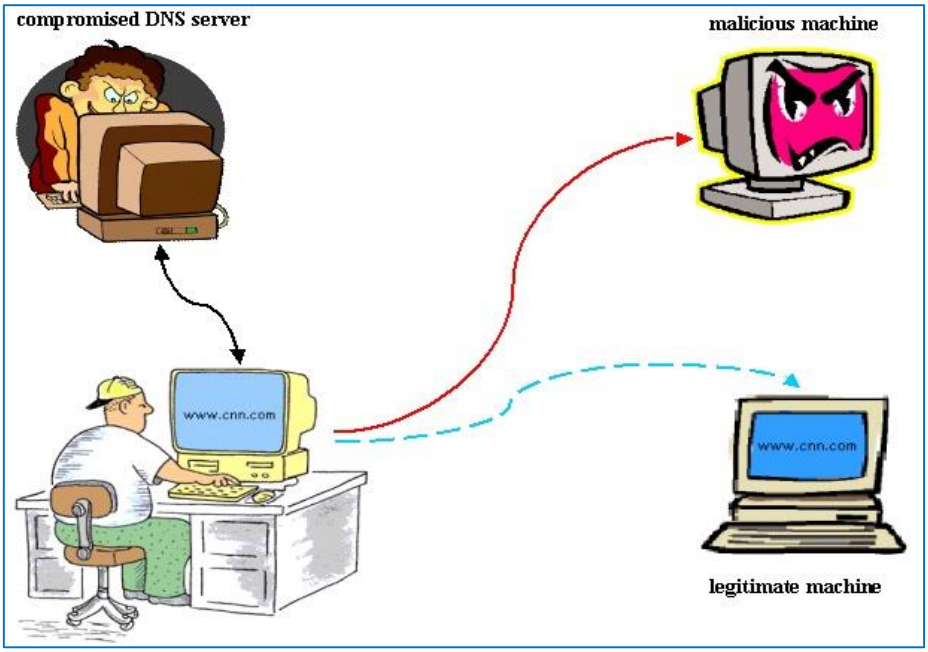
Будьте обережні при отриманні несподіваного повідомлення по електронній пошті від благодійної організації з проханням пожертвувати гроші. Не відкривайте ніякі вкладення і не переходьте ні по яких посиланнях. Введіть вручну веб-адресу благодійної організації в адресному рядку браузера і, перш ніж жертвувати гроші, переконайтеся в тому, що запит є законним.

б) Фармінг – це набагато складніша технологія. Він полягає в зміні змісту DNS (Domain Name Server), або через налаштування протоколу TCP/IP, або через файл Imhost, діючий як локальний кеш серверних імен для того, щоб при спробі користувача відкрити легітимні сайти, перенаправляти його на фальсифіковані версії. Більш того, якщо при користуванні Інтернетом для збереження анонімності жертва використовує проксі, повідомлення примушує користувачів перейти за посиланням, яке приведе їх на веб-сайт, де вони повинні ввести свої конфіденційні дані, які зазвичай нібито з метою їх підтвердження потрібно повторно активувати свій рахунок і т.ін.

Звичайно ж, посилання веде не на реальний сайт компанії, а на веб-сайт, створений шахраями, що імітує корпоративний імідж фінансової або банківської організації. Відображувана веб-адреса, як правило, містить назву легітимної установи, щоб користувачі не запідозрили нічого поганого.

Оскільки повідомлення розсилаються в масовому порядку, деякі з одержувачів дійсно виявляться клієнтами компанії. У повідомленні йдеться про те, що з причини деяких аспектів безпеки, користувачеві необхідно відвідати веб-сайт і підтвердити свої дані: ім'я користувача, пароль, номер кредитної картки, PIN-код, номер картки соціального страхування та ін.

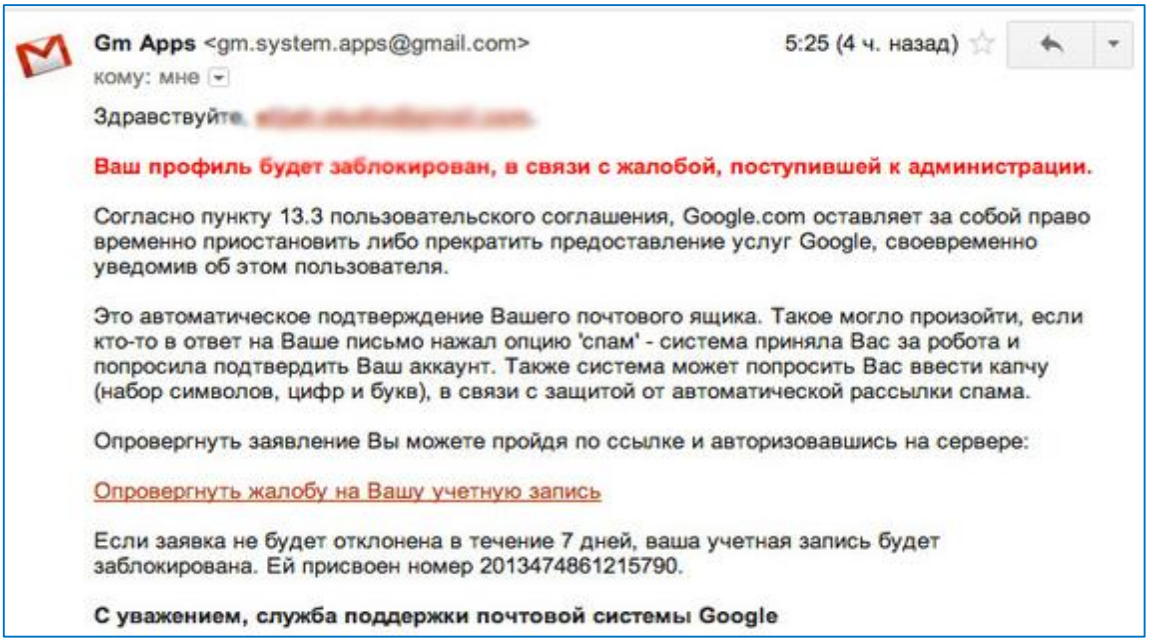
Коли користувач вводить свої конфіденційні дані, ці дані зберігаються в базі, а далі шахраї використовують отриману інформацію для входу на Ваш рахунок і всі кошти виявляться у них в руках .



Схематичне зображення процесу фармінгу

Яку ціль переслідують зловмисники?

Ціллю шахраїв є отримання ваших особистих даних з метою доступу до рахунку в банку, «електронних грошей» тощо. Разом з цим, слід пам'ятати, що вони можуть отримати доступ до ваших коштів не лише через ваші облікові дані у банку або платіжній системі.



Gm Apps <gm.system.apps@gmail.com> 5:25 (4 ч. назад)

кому: мне

Здравствуйте,

Ваш профиль будет заблокирован, в связи с жалобой, поступившей к администрации.

Согласно пункту 13.3 пользовательского соглашения, Google.com оставляет за собой право временно приостановить либо прекратить предоставление услуг Google, своевременно уведомив об этом пользователя.

Это автоматическое подтверждение Вашего почтового ящика. Такое могло произойти, если кто-то в ответ на Ваше письмо нажал опцию 'спам' - система приняла Вас за робота и попросила подтвердить Ваш аккаунт. Также система может попросить Вас ввести капчу (набор символов, цифр и букв), в связи с защитой от автоматической рассылки спама.

Опровергнуть заявление Вы можете пройдя по ссылке и авторизовавшись на сервере:

Опровергнуть жалобу на Вашу учетную запись

Если заявка не будет отклонена в течение 7 дней, ваша учетная запись будет заблокирована. Ей присвоен номер 2013474861215790.

С уважением, служба поддержки почтовой системы Google

Даний фішинговий лист направлений на крадіжку облікових даних електронної пошти

Так, часто при застосуванні фішингу ціллю є інформація про особисті дані, прямо не пов’язані з вашим рахунком. Такою інформацією можуть бути: пароль до вашої скриньки електронної пошти, пароль до облікового запису у соціальних мережах тощо.

Отримані зловмисниками особисті дані можуть використовуватися у різних цілях. Найбільш «невинною» є використання вашої поштової скриньки для розсилки спам-листів. Разом з цим, наслідки отримання зловмисниками доступу до вашої поштової скриньки можуть бути й більш серйозними.

Так, достатньо часто саме до поштової скриньки прив’язано ваш обліковий запис у платіжних системах, у ній можуть міститись дані для доступу до вашого банківського рахунку. Нарешті, доступ до вашої особистої переписки може бути використаний з метою шантажу.

Яким чином розпізнати фішинговий лист?

Хоча зловмисники використовують різні підходи для заманювання на підроблені сайти, в цілому можна виділити декілька особливостей листа, що мають викликати у вас підозру:

– банки **ніколи** не запитують персональні дані платіжної картки через листи, надіслані електронною поштою;

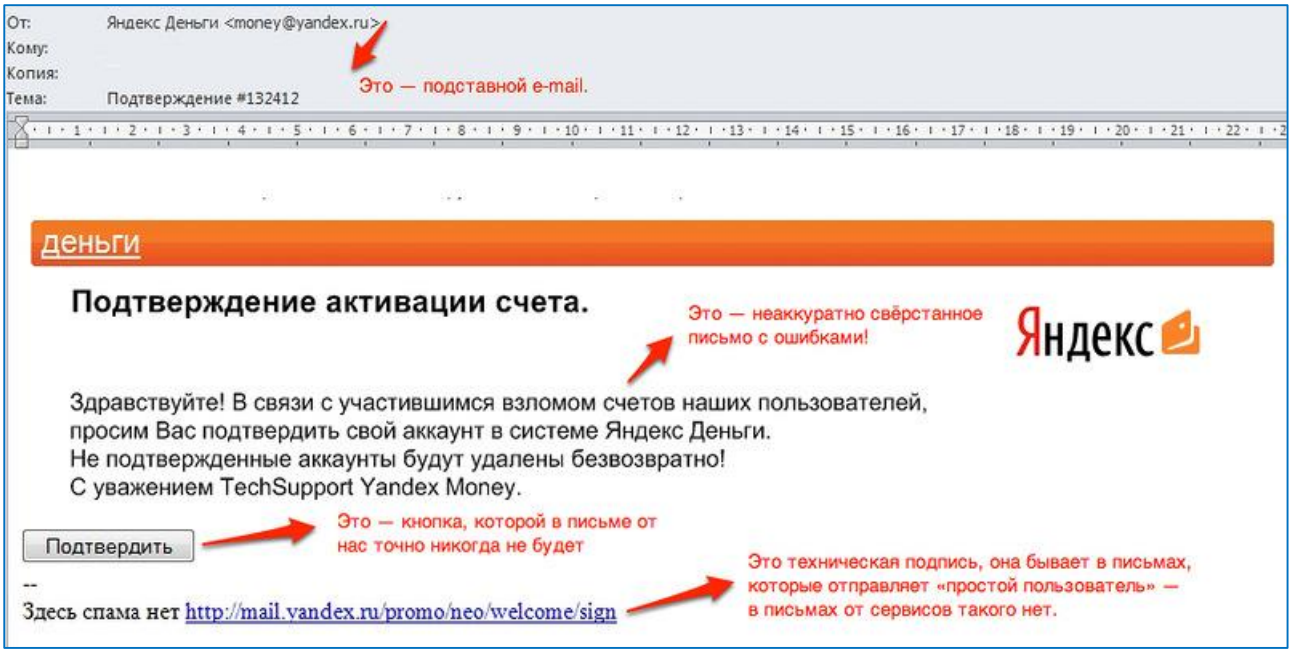
– часто (але не завжди) фішингові листи містять граматичні помилки;

– звернення може бути знеособленим (напр., «Шановний клієнт!»);

– тон фішингових листів, як правило, тривожний, а самі вони закликають до негайних дій (інакше рахунок буде заблокований/гроші не отримані/дані втрачені тощо);

– лист містить обіцянки великої грошової вигоди з мінімальними зусиллями або зовсім без них;

– у листі є запити про пожертвування від особи благодійних організацій після повідомлень в новинах про стихійні лиха.



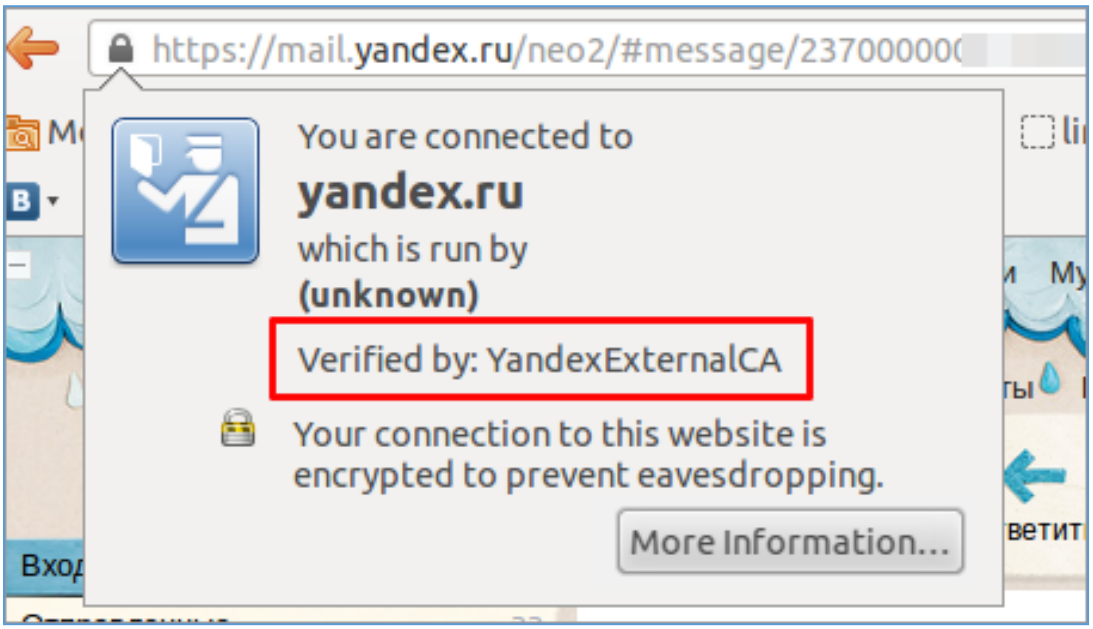
Приклад ідентифікації фішингового листа

Виконайте наступні дії, щоб мінімізувати збиток, якщо ви припускаєте, що відповіли на фішингові повідомлення, вказавши свою особисту чи фінансову інформацію, або ввели цю інформацію на шахрайському веб-сайті

1. Змініть паролі або PIN-коди для всіх своїх облікових записів в Інтернеті, які могли бути піддані небезпеці.
2. Помістіть попередження про шахрайство в свої звіти за кредитами. Якщо ви не знаєте, як це зробити, зверніться в банк або до фінансового консультанта.
3. Зверніться в банк або в Інтернет-магазин безпосередньо. Не переходьте за посиланням у шахрайському повідомленні електронної пошти.
4. Якщо вам стало відомо про доступ або про відкриття рахунків шахраями, закрийте ці рахунки.
5. Кожен місяць переглядайте виписки з банку і звіти за операціями з кредитною картою, звертаючи уваги на незрозумілі витрати або запити, які ви не ініціювали.

Запобіжні заходи, які в змозі здійснити кожний користувач

1. Особисті дані у жодному разі не можна вводити в анкетах, що надсилаються електронною поштою. Це стосується не лише даних вашої платіжної картки або вашого банківського рахунку, але й паролів до скриньки електронної пошти, облікових записів у соціальних мережах тощо. Подібні дані можна вводити лише на сайтах із захищеним з'єднанням. Такі сторінки мають префікс https:// (замість звичного http://) на початку адреси, а біля адреси з'являється символ у вигляді замочка.



Приклад захищеного з'єднання (при натисканні на символ замочка з'являється інформація про сертифікат безпеки)

2. Слід пам'ятати, що можливим є маскування зловмисниками справжньої адреси сайту, тому не варто вводити свої персональні дані на сторінках, на які ви перейшли за посиланням (у найпростіших випадках у тому, що адреса несправжня, можливо переконатись лише навівши курсор на адресу посилання; під курсором висвітиться справжня адреса).

Адреса, показана на посиланні не відповідає адресі, на яку воно перенаправляє

3. Регулярно перевіряйте стан свого банківського рахунку, особливо якщо до нього прив’язані платіжні картки.

4. Регулярно змінюйте паролі доступу до електронної пошти, інших користувацьких записів.

5. Ніколи не завантажуйте і не переходьте за посиланнями, отриманими від невідомого джерела.

6. Ніколи не надавайте жодних особистих даних, що не відносяться до роботи, наприклад номер соціального страхування, номер кредитної картки, дату народження, домашню адресу та відомості про сімейний стан по Інтернету, по електронній пошті, по телефону, у факсі або в своєму резюме.

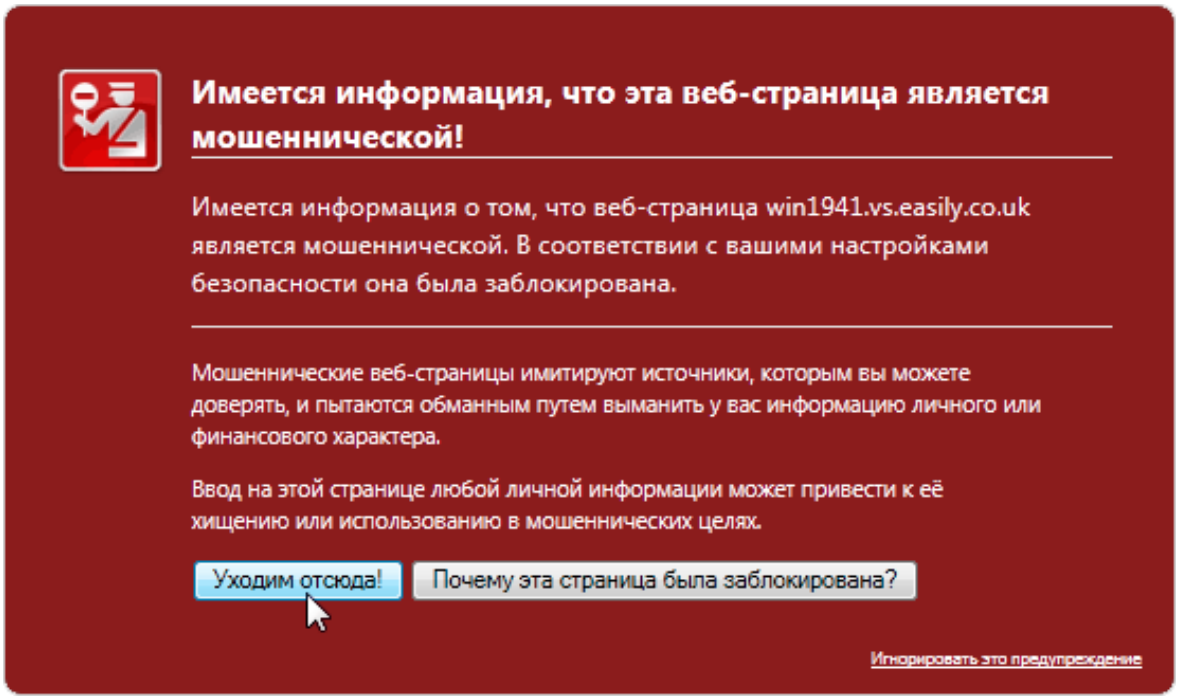
7. Публікуйте своє резюме на сайті пошуку роботи, на якому допускаються тільки перевірені роботодавці, де проводиться їх сканування, а також діє політика дотримання конфіденційності. Якщо потенційний наймач або роботодавець зажадає перевірку біографічних даних, погоджуйтеся на це тільки після особистої зустрічі в компанії в звичайні години роботи.

Важливим елементом захисту від цього виду шахрайства є використання якісного програмного забезпечення: Інтернет-браузера та антивірусних програм

Більшість Інтернет-браузерів, тобто програм для перегляду Інтернет-сторінок, мають вбудовані системи захисту від фішингу.

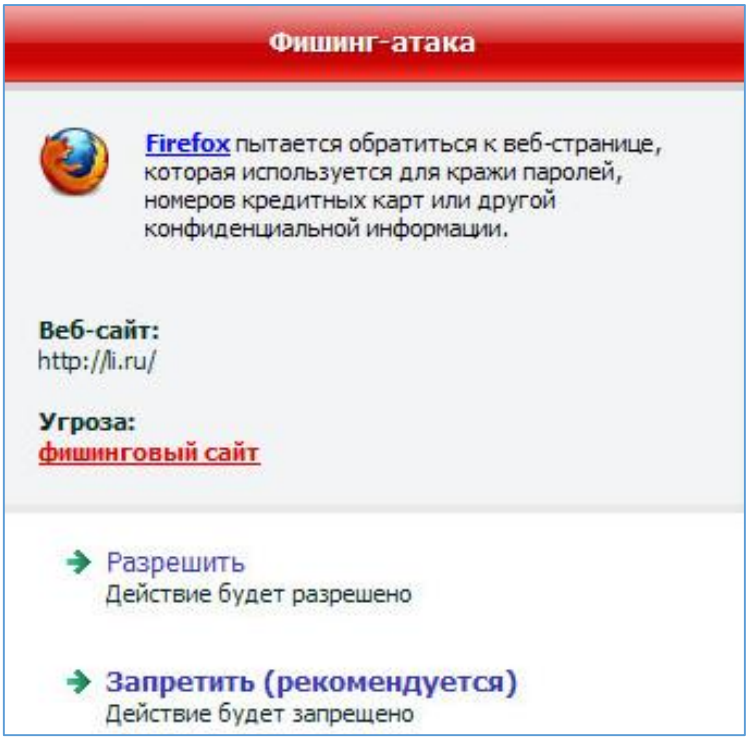
Коли така система увімкнена (у більшості браузерів ця функція обрана за замовчуванням) браузер перед переходом перевіряє сертифікати сайту, відповідність фактичної та вказаної у сертифікаті адреси, наявність сайту у «чорних списках» сторінок, що поширюють зловмисне програмне забезпечення або створені для фішингу тощо.

Якщо сайт не відповідає вимогам безпеки, браузер попереджує про це користувача. У зв’язку з цим, необхідно періодично оновлювати браузер, яким ви користуєтесь. Справа в тому, що у будь-якому програмному забезпеченні існують вразливі місця, якими й користуються зловмисники. Кожна нова версія браузера виправляє відомі проблеми, а тому забезпечує безпеку користувача краще.



Приклад повідомлення Інтернет-браузера про фішинговий сайт

Антивірусне програмне забезпечення спрямоване на протидію всім типам зловмисного програмного забезпечення, більшість антивірусних програм мають опцію антифішингового захисту. Програма попереджує користувача про підозрілий характер сайту (у цьому випадку, однак, фільтр працює надійніше). Іншою корисною функцією є перевірка листів, що надходять на поштову скриньку: відбувається фільтрація як власне фішингових листів, так і листів, що містять віруси.



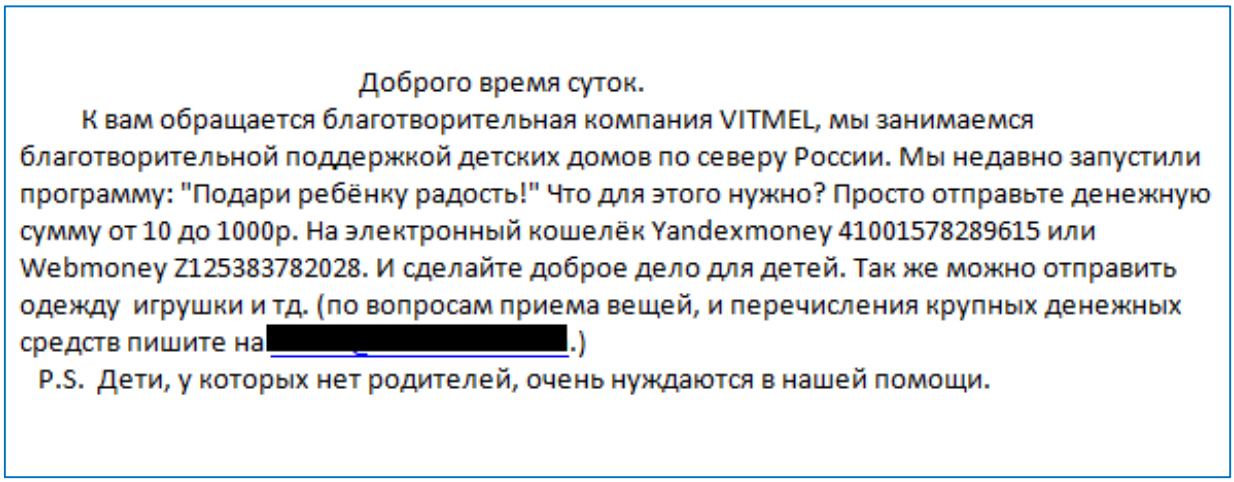
Приклад повідомлення антивірусної програми про фішингову атаку

1.3.2. Шахрайські листи що пов’язані з благодійністю та акціями?

Інтернет-жебрацтво

Це електронні листи нібито від благодійних організацій або людей, які потребують допомоги. Насправді такі листи або є в чистому вигляді блефом, або в них знаходяться посилання на реальні організації та фонди, але зазначені реквізити для переказу грошей належать шахраям.

Пам’ятайте, благодійні організації не розсилають спам, у них є інші методи для залучення інвестицій. Якщо ви все-таки хочете перевірити інформацію, яка надана в листі, знайдіть адресу відповідної організації, зателефонуйте туди і уточніть, яким чином можна перевести гроші.



Доброго время суток.

К вам обращается благотворительная компания VITMEL, мы занимаемся благотворительной поддержкой детских домов по северу России. Мы недавно запустили программу: "Подари ребёнку радость!" Что для этого нужно? Просто отправьте денежную сумму от 10 до 1000р. На электронный кошелёк Yandexmoney 41001578289615 или Webmoney Z125383782028. И сделайте доброе дело для детей. Так же можно отправить одежду игрушки и тд. (по вопросам приема вещей, и перечисления крупных денежных средств пишите на [redacted].)

P.S. Дети, у которых нет родителей, очень нуждаются в нашей помощи.

Приклад фіктивного благодійного листа

Нігерійські листи

Види цього шахрайства досить різноманітні. Найбільш часто листи відправляються від імені колишнього короля, президента, високопоставленого чиновника або мільйонера з проханням про допомогу в банківських операціях, пов'язаних з переведенням грошей з Нігерії або іншої країни за кордон,

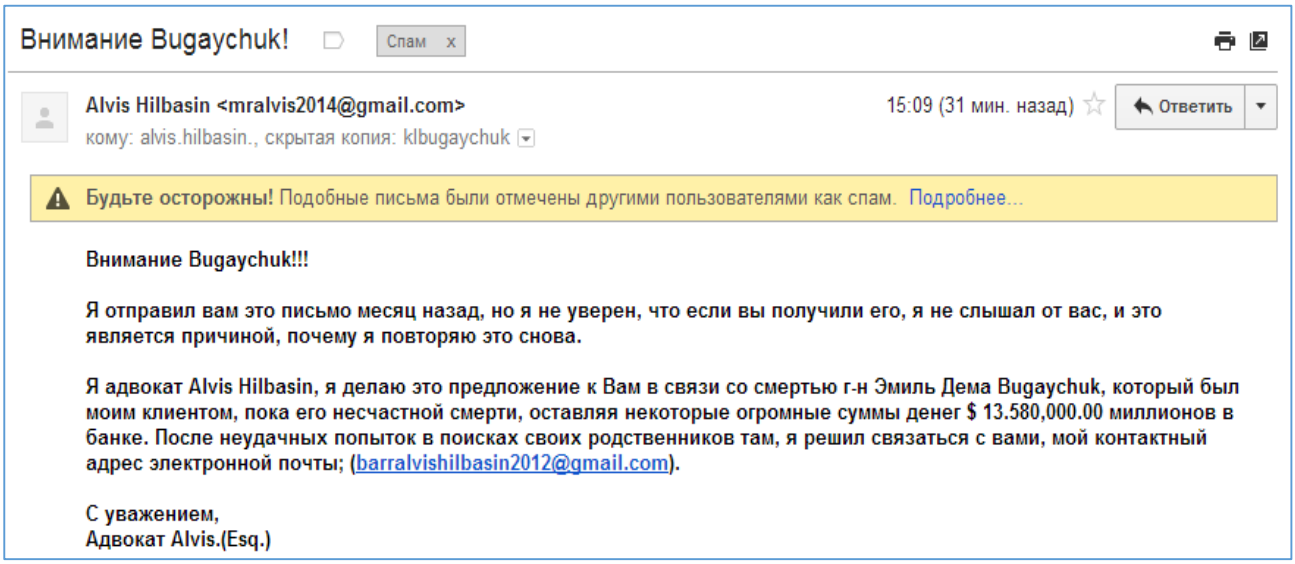
отриманням спадщини і т. ін., нібито оподатковуваних великим податком. Інший поширений варіант – листи, нібито, від працівника банку або від чиновника, котрий дізнався про недавню смерть дуже багатої людини «з таким же прізвищем», як у одержувача листа, з пропозицією надати допомогу в отриманні грошей з банківського рахунку цієї людини.

Є листи нібито від дочки убитого повстанцями політика, яка нібито знаходиться в таборі біженців і просить допомогти їй звідти вибратися, для чого знову-таки потрібні банківські операції.

Від одержувачів таких листів у будь-якому випадку потрібно одне і те ж – надати допомогу в проведенні різних банківських операцій. Зрозуміло, не за «спасибі»: мова завжди йде про величезні суми грошей (мільйони доларів США), а «помічникові» покладається чималий відсоток.

За такою схемою з «жертвами» працюють справжні «професіонали». Перед початком «операції» вони орендують офіси, створюють власні сайти, при підготовці документів використовують печатки та бланки великих фірм, які складно відрізнити від справжніх, іноді навіть налагоджують контакти з урядовими організаціями. Якщо одержувач листа захоче перевірити «легенду», вигадану шахраями, то навряд чи зможе виявити хоч якісь протиріччя.

У наступних листах у «помічника» просять переказувати гроші: на банківські збори, хабарі посадовим особам та інші «поточні витрати». Підсумок афери завжди однаковий: протягом якогось часу наївний громадянин буде набивати гаманці шахраїв, але обіцяного гонорару не дочекається ніколи.



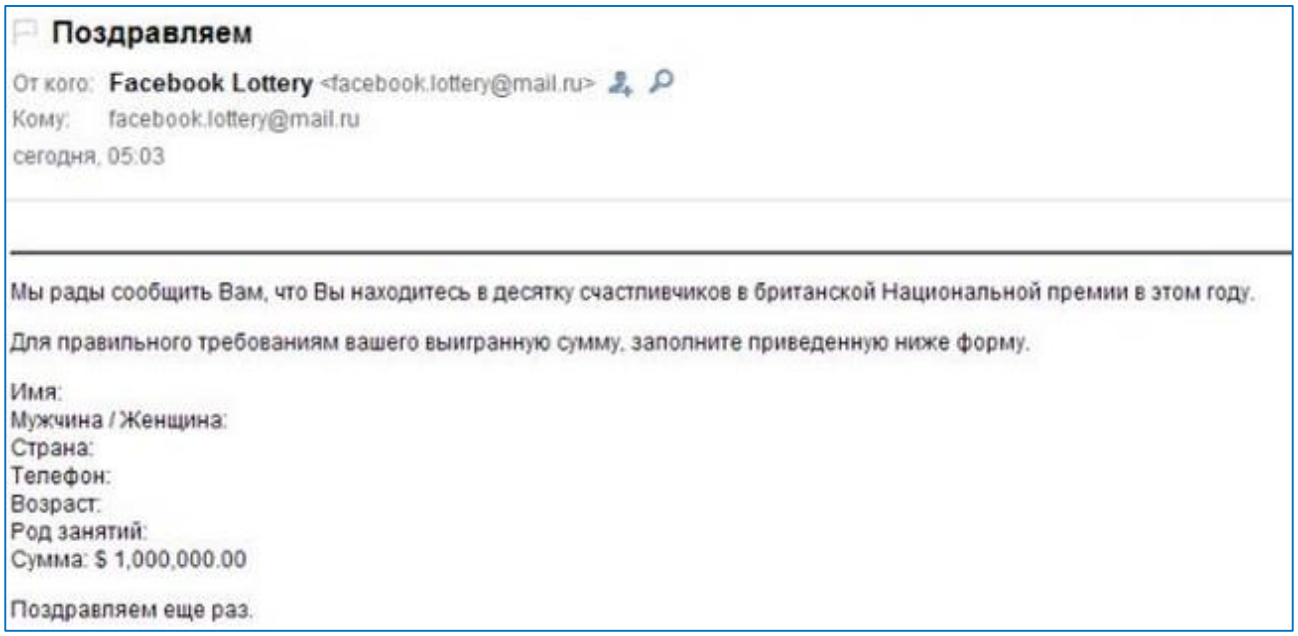
Приклад «нігерійського листа»

Інтернет лотереї

Одна з найпопулярніших схем роботи шахраїв – великий виграш в Інтернет-лотерею. Адресат отримує листа, де йдеться, що адреса його електронної пошти заочно брала участь в якійсь лотереї і була вибрана з кількох мільйонів їй подібних. Власнику поштової скриньки в якості призу тепер належить велика сума грошей.

Далі людину, якщо вона відповість, практично «завалюють» листами з ксерокопіями виграшних сертифікатів і, врешті-решт, запитують, яким чином вона хотів би отримати виграні гроші. Погоджуються, як правило, на банківський переказ.

Далі, щоб остаточно увійти в довіру «жертви», шахрай може вислати копію паспорта банківського працівника, який займається переказом виграшу (зрозуміло, підроблену). В одному з листів жертва отримує виписку з законодавства: виявляється, щоб виключити можливість розкрадання призового фонду, ніхто і ні за яких умов не може взяти з призових грошей ні копійки. Але ж треба оплатити проїзд кур'єра в країну, де живе громадянин, роботу адвоката і так далі. У наступному листі «організатор лотереї» повідомляє, що часу на отримання виграшу залишається зовсім мало – весь призовий фонд може перейти у власність держави. Потім Інтернет-користувач власноруч переводить йому певну суму грошей. Через деякий час будь-який зв'язок з шахраєм пропадає, а ніякого виграшу, зрозуміло, просто не існувало.



Поздравляем

От кого: **Facebook Lottery** <facebook.lottery@mail.ru>
Кому: facebook.lottery@mail.ru
сегодня, 05:03

Мы рады сообщить Вам, что Вы находитесь в десятку счастливчиков в британской Национальной премии в этом году.

Для правильного требованиям вашего выигранную сумму, заполните приведенную ниже форму.

Имя:
Мужчина / Женщина:
Страна:
Телефон:
Возраст:
Род занятий:
Сумма: $ 1,000,000.00

Поздравляем еще раз.

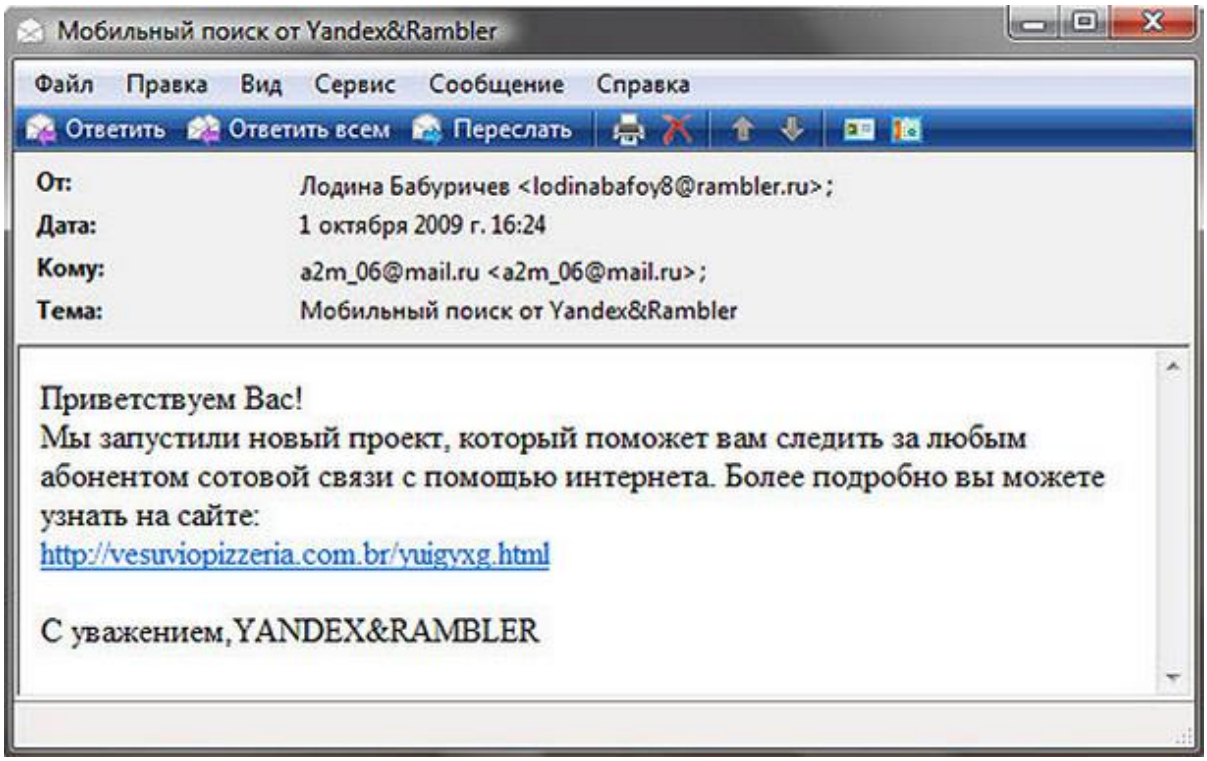
Приклад спаму про участь у лотереї

1.3.3. Спам та шкідливе програмне забезпечення

Спам (англ. spam) – це масова незапитуваної розсилання електронних повідомлень, що рекламують послуги або продукти.

Яким чином поширюється спам?

Більшість спамерів використовують масову розсилку для розповсюдження реклами, продукції або різних вірусів. У першу чергу, термін «спам» відноситься до електронних листів. Незапитуваної розсилка у програмах обміну миттєвими повідомленнями називається SPIM (від англ. Spam over IM). Також, відомий термін SPIT (від англ. Spam over IT) - спам, поширюваний через IP-телефонію (наприклад, через форуми користувачів Skype).



Приклад спаму

Як спам впливає на роботу комп'ютера?

Незважаючи на те, що спам може і не містити віруси або інші шкідливі програми, це викликає незручність і призводить до зниження продуктивності, так як Ви щодня змушені відстежувати і видаляти небажані повідомлення. У великих організаціях велика кількість спаму може викликати перевантаження поштового сервера, що впливає на ефективність роботи. У крайніх випадках спамери використовують відомі уразливості в програмному забезпеченні чи комп'ютерні віруси для того, щоб захопити управління над великою кількістю комп'ютерів, підключених до Інтернету, і вже їх використовувати для розсилки повідомлень іншим користувачам.

Як захистити себе від спаму?

1. Перед тим, як розміщувати будь-де адресу своєї електронної пошти, ознайомтеся з політикою конфіденційності ресурсу. Кожен сайт повинен надати посилання на розділ, присвячений політиці конфіденційності, де пояснюється, яким чином будуть використані надані дані.
2. У процесі реєстрації акаунту, переконайтеся, що всі налаштування, встановлені за замовчуванням (наприклад, підписка на розсилку), відключені.
3. Відповідаючи на спам-листи або відкриваючи посилання, надіслані в них, Ви підтверджуєте, що Ваша електронна адреса є робочою. Надалі, Ви будете отримувати ще більшу кількість небажаної кореспонденції. Буде правильніше повністю ігнорувати подібні повідомлення і видаляти їх.
4. Для захисту Вашої електронної пошти від великої кількості спаму, зареєструйте ще один e-mail і використовуйте його виключно для покупок через Інтернет, чатів та інших онлайн-сервісів.

Що таке шкідливе програмне забезпечення?

Malware (від англ. «Malicious software»: Mal icious – зловмисний і Soft Ware – програмне забезпечення) – загальноприйнятий термін, використовуваний для позначення будь-якого програмного забезпечення, спеціально створеного для

того, щоб завдавати шкоди окремому комп’ютеру, серверу, або комп’ютерній мережі.

Шкідливі програми являють собою широку категорію програмного забезпечення. Вони встановлюються без Вашого дозволу і впливають на роботу Вашого комп'ютера. Найбільш поширеними видами шкідливих програм є трояни, черв’яки і віруси.

Троян - шкідлива програма, використовувана зловмисником для збору інформації, її руйнування або модифікації, порушення працездатності комп'ютера або використання його ресурсів в непристойних цілях.

Комп'ютерний вірус – різновид комп’ютерної програми, відмітною особливістю якої є здатність до розмножения (самореплікації). На додаток до цього він може пошкоджувати або повністю знищувати дані, підконтрольні користувачу, від імені якого була запущена заражена програма.

Мережевий черв’як – різновид самовідтворюваної комп'ютерної програми, що розповсюджується в локальних і глобальних комп'ютерних мережах. На відміну від комп'ютерних вірусів черв'як є самостійною програмою. Trackware – нова варіація шкідливої програми, яка відстежує і реєструють дії, вироблені на комп'ютері.

Яким чином шкідливі програми проникають на комп'ютер користувача?

Шкідливі програми, найчастіше, проникають на комп'ютер через Інтернет або електронну пошту. Якщо Ви зробите помилку в URL-адресі або випадково натиснете на невідомі посилання, то можете потрапити на небезпечні сайти з «агресивним» змістом або шкідливими програмами.

Як шкідливі програми впливають на роботу комп'ютера?

Симптомами зараження шкідливою програмою є спливаючі вікна, зниження працездатності системи або перенаправлення запитів в браузері на небажані сайти.

Шкідливі програми впливають на нормальне функціонування системи, що може призвести до відмови в обслуговуванні, заміні даних і зниження

пропускної здатності мережі. Крім того, комп’ютер буде неможливо вимкнути або перезавантажити.

Як захистити комп'ютер від шкідливих програм?

– шкідливі програми часто поширюються в додатку з іншими файлами, так що не відкривайте вкладення електронної пошти, відправлені з невідомих Вам ресурсів;

– ніколи не приймайте файли від незнайомих Вам користувачів, а також проявляйте обережність, коли відкриваєте файли з розширенням: AVI, EXE або JPG;

– якщо Ви підозрюєте, що Ваш комп’ютер заражений шкідливою програмою призупиніть будь-яку діяльність, яка пов’язана з використанням логінів, паролів та іншої конфіденційної інформації;

– використовуйте антивірусне програмне забезпечення для захисту Вашої системи від можливих онлайн-загроз, регулярно оновлюйте його;

– переконайтеся, що Ваша антивірусна програма оновлена, сканує комп'ютер і видаляє всі програми, які визначаються як шкідливі;

– під час користування Інтернетом, включайте брандмауер;

– перш ніж відкривати скачані файли, перевіряйте їх за допомогою антивірусної програми.

1.3.4. Шпигунське програмне забезпечення

Spyware (від англ. Spy - шпигун і Soft Ware – програмне забезпечення) – це несанкціоновано встановлений програмний продукт, метою якого є приховане відстеження поведінки користувача в мережі.

Також, подібні програми використовуються для збору різних типів особистої інформації:

– звичка користування Інтернетом і відвідувані сайти (Tracking Software);

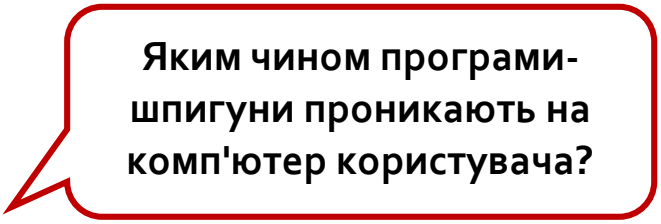
– контроль натискань клавіш на клавіатурі комп'ютера (Keyloggers);

– контроль скріншотів екрану монітора комп'ютера (Screen Scraper);

– несанкціонований віддалений контроль і управління комп'ютерами (Remote Control Software);

– несанкціонований аналіз стану систем безпеки (Security Analysis Software).

Spyware можуть навіть міняти установки в комп'ютері для несанкціонованого внесення змін в операційну систему, результатом чого є зниження швидкості з'єднання з Інтернетом або втрата з'єднання як такого, відкривання інших домашніх сторінок або видалення тих чи інших програм.



Часто Spyware поширюються в комплекті з іншим програмним забезпеченням, безкоштовними пробними (trial) версіями програм і з деякими викачуваними продуктами. Також, програми-шпигуни потрапляють в систему шляхом обману користувача або через уразливість системи.

Деякі типи Spyware відключають брандмауер і антивірусні програми і / або знижують установки безпеки браузера, таким чином, роблячи систему неприкритою для подальшого шкідливого програмного забезпечення. При видаленні якого-небудь компоненту Spyware, програма автоматично його відновлює.

У доповнення до руйнування системи Вашого комп'ютера, програми-шпигуни можуть запускати спливаючі рекламні вікна, впливати на продуктивність процесора і ефективність роботи інших програм. Надмірна кількість spyware-програм на Вашому комп'ютері може призвести до частих збоїв і зниження швидкості роботи системи.

Як захистити комп'ютер від spyware?

– ознайомтесь з правилами безпечного серфінгу та інформацією про нові загрози;

– запустіть антишпигунські і антивірусні програми для очищення комп'ютера;

– переконайтеся, що на Ваш браузер і операційну систему встановлені останні оновлення;

– увімкніть автоматичне оновлення програмного забезпечення;

– встановіть у браузері високий рівень безпеки та конфіденційності інформації;

– ігноруйте спливаючі рекламні вікна.

1.3.5. Кібербулінг, кібермоббінг, секстінг, грумінг

Англійське слово булінг (bullying, від bully – забіяка, грубіян) означає залякування, приниження, цькування, фізичний чи психологічний терор, спрямований на те, щоб викликати в іншого страх і тим самим підпорядкувати його собі.

Кібербулінг – переслідування повідомленнями, що містять образи, агресію, залякування; соціальне бойкотування за допомогою різних Інтернет-сервісів.

Основним майданчиком для кібербулінгу останнім часом є соціальні мережі. У них можна ображати людину не тільки за допомогою повідомлень – нерідкі випадки, коли сторінку жертви зламують (або створюють підроблену на її ім'я), де розміщують брехливий і принизливий контент.

Прикладом кібербуллінгу може бути випадок, що стався на Закарпатті, де школярі зацькували у соціальній мережі свою однокласницю – 14-річну А. Фіцай до самогубства.

Чим кібербулінг відрізняється від звичайного залякування?

Образливі ситуації найчастіше відбуваються у вигляді цілого ряду неприємних інцидентів, що мають місце, як при особистому спілкуванні, так і в кіберпросторі. Звичайне залякування – це конфронтація при особистому спілкуванні і часто віч на віч, з використанням погроз і фізичного насильства. Кібербулінг ж практикується в електронному вигляді, і провокативні матеріали можуть бути швидко і широко поширені, при цьому це безперервний процес, що залучає безліч людей.

Чим кібербулінг відрізняється від секстінгу?

Секстінг – це пересилання фотографій або повідомлень сексуального характеру, яке зазвичай, відбувається між двома людьми, пов’язаними особистими відносинами. Секстінг можна розглядати як кібербулінг в тому випадку, якщо такі фотографії здобуті обманним шляхом, а потім поширені з метою шкоди репутації жертви.

Чим кібербулінг відрізняється від кібермоббінгу?

Кібербулінг часто плутають з мобінгом, або масовим цькуванням (від mob – натовп), хоча насправді агресивна поведінка, яке позначається цими двома поняттями, має різні соціально-психологічні механізми.

Зазвичай під мобінгом розуміють груповий психологічний терор у вигляді непрямго або прямого цькування людини в колективі. У широкому сенсі мобінг являє собою систематичні, повторювані протягом тривалого часу, образи, приниження гідності іншої людини, наприклад, у школі, на робочому місці, і також через Інтернет (кібермоббінг).

Типові дії, здійснювані при моббінгу – це поширення завідомо неправдивої інформації (чуток і пліток) про людину, глузування і провокації, прямі образи і залякування, соціальна ізоляція (бойкот і демонстративне ігнорування), нападки, що ущемляють честь і гідність людини, заподіяння матеріальної або фізичної шкоди .

Причини здійснення кібермоббінгу

– страх: щоб не стати жертвою мобінгу особи часто примикають до активної, імовірно сильної групи;

– завоювання визнання: потреба «виділитися», бути на виду, завоювати вплив і престиж в групі;

– міжкультурні конфлікти: національні відмінності в культурі, у традиціях, у мові, нетипова зовнішність;

– нудьга: наприклад, від нудьги негативно прокоментувати чиюсь фотографію;

– демонстрація сили: потреба показати свою перевагу;

– комплекс неповноцінності: можливість «ухилятися» від комплексу або проектувати його на іншого.

Які типи кібербулінгу виділяють дослідники?

1. **Перепалки, або флеймінг** – обмін короткими емоційними репліками між двома і більше людьми, розгортається зазвичай в публічних місцях Інтеренет. Іноді перетворюється на затяжний конфлікт – «холивар» (holywar – священна війна). На перший погляд, флеймінг – боротьба між рівними, але за певних умов вона може перетворитися на нерівноправний психологічний терор. Несподіваний випад може викликати у жертви сильні емоційні переживання.

2. **Нападки, постійні виснажливі атаки (harassment)** – повторювані образливі повідомлення, спрямовані на жертву (наприклад, сотні sms на мобільний телефон, постійні дзвінки), з перевантаженням персональних каналів комунікації. Зустрічаються також в чатах і форумах, в онлайн-іграх цю технологію найчастіше використовують гріфери (grieffers) – група гравців, що мають на меті не перемогу, а руйнування ігрового досвіду інших учасників.

3. **Наклеп (denigration)** – поширення образливої та неправдивої інформації. Текстові повідомлення, фото, пісні, які часто мають сексуальний

характер. Жертвами можуть бути не тільки окремі підлітки – часом трапляються розсилки списків («хто є хто в організації», «хто з ким спить»), створюються спеціальні «книги для критики» (slam books).

4. **Самозванство, перевтілення в певну особу (impersonation)** – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до акаунтів у соціальних мережах, в блозі, пошті, системі миттєвих повідомлень, або створює свій акаунт з аналогічним никнеймом і здійснює від імені жертви негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відома відправляють друзям провокаційні листи.

5. **Омана (шахрайство),** виманювання конфіденційної інформації та її поширення (outing & trickery) – отримання персональної інформації та публікація її в Інтернеті або передача тим, кому вона не призначалася.

6. **Відчуження (ізоляція).** Будь-якій людині притаманне бажання бути включеним до групи. Виключення ж з групи сприймається як соціальна смерть. Чим більшою мірою людина виключається з взаємодії, тим гірше він себе почуває, і тим більше падає його самооцінка. У віртуальному середовищі це може призвести до повного емоційного руйнування дитини. Онлайн-відчуження можливе в будь-яких типах середовищ, де використовується захист паролем, формується список небажаної пошти або списку друзів.

7. **Кіберпереслідування** – приховане вистежування жертви з метою організації нападу, побиття, згвалтування і т.ін.

8. **Хеппіслепінг (Happy Slapping – радісне побиття)** – назва походить від випадків в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефону. Зараз ця назва закріпилася за будь-якими відеороликами із записами реальних сцен насильства. Ці ролики розміщують в Інтернеті, де їх можуть переглядати тисячі людей, без згоди жертви.

Спілкуючись в мережі, діти можуть знайомитися, спілкуватися і додавати в «друзі» зовсім невідомих їм у реальному житті людей. У таких ситуаціях є небезпека розголошення дитиною особистої інформації про себе і свою сім'ю. Також користувач ризикує піддатися образам, залякуванню і домаганням.

Особливо небезпечним може стати грумінг – встановлення дружніх відносин з дитиною з метою особистої зустрічі, вступу з нею у сексуальні

відносини, шантажу та експлуатації. Такі знайомства найчастіше відбуваються в чаті, на форумі або в соціальній мережі.

Спілкуючись особисто зловмисник, найчастіше представляється однолітком, входить в довіру до дитини, а потім намагається дізнатися особисту інформацію (адреса, телефон тощо) і домовитися про зустріч.

Іноді такі люди виманюють у дітей інформацію, якою потім можуть шантажувати дитину, наприклад, просять надіслати особисті фотографії або провокують на непристойні дії перед веб-камерою.

Як запобігти проявам кібербулінгу?

1. Поясніть дітям, що при спілкуванні в Інтернеті вони повинні бути дружелюбними з іншими користувачами. Ні в якому разі не варто писати різкі і образливі слова - читати грубості так само неприємно, як і чути.

2. Навчіть дітей правильно реагувати на образливі слова чи дії інших користувачів. Не варто спілкуватися з агресором, і тим більше намагатися відповісти йому тим же. Можливо варто взагалі покинути даний ресурс і видалити звідти свою особисту інформацію, якщо не виходить вирішити проблему мирним шляхом. Кращий спосіб зіпсувати хулігану його витівку – відповідати йому повним ігноруванням.

3. Якщо у вас є інформація, що хтось із друзів або знайомих вашої дитини піддається булінгу або кібербулінгу, то повідомьте про це класному керівнику або шкільного психологу – необхідно вжити заходів щодо захисту дитини.

4. Зв’яжіться з батьками кривдника і чітко дайте їм зрозуміти, що переслідування повинно припинитися. Пред’явіть електронні докази.

5. Поясніть дітям, що особиста інформація, яку вони викладають в Інтернеті (домашня адреса, номер мобільного або домашнього телефону, адресу електронної пошти, особисті фотографії) може бути використана агресорами проти них.

6. Допоможіть дитині знайти вихід із ситуації - практично на всіх форумах і сайтах є можливість заблокувати кривдника, написати скаргу модератору або адміністрації сайту, зажадати видалення сторінки.

7. Підтримуйте довірчі відносини з вашою дитиною, щоб вчасно помітити, якщо на її адресу почне надходити агресія або загрози. Спостерігайте за її настроєм під час і після спілкування з ким-небудь в Інтернеті.

8. Переконайтеся, що образи (булінг) з мережі не перейшли в реальне життя. Якщо загрози є досить серйозними, стосуються життя або здоров'я

дитини, а також членів вашої родини, то ви маєте право на захист з боку правоохоронних органів.

9. Збережіть всі можливі свідчення того, що відбувається (скріншоти екрану, електронні листи, фотографії тощо).

10. Зберігайте спокій - ви можете ще більше налякати дитину своєю бурхливою реакцією на те, що вона вам розповіла і показала. Головним завданням є емоційна підтримка дитини. Потрібно дати їй впевненість у тому, що проблему можна подолати. Ніколи не карайте і не обмежуйте дії дитини у відповідь на його визнання.

Як запобігти проявам грумінгу?

1. Зверніть увагу, кого дитина додає до себе «в друзі», з ким вважає за краще спілкуватися в мережі – з однолітками або людьми старше себе.

2. Поясніть дитині, що не можна розголошувати в Інтернеті інформацію особистого характеру (номер телефону, домашню адресу, назву / номер школи і т. д.), а також пересилати віртуальним знайомим свої фотографії або відео.

3. Поясніть дитині, що не можна ставити на «аватар» або розміщувати в мережі фотографії, за якими можна судити про матеріальне благополуччя сім'ї, а також недобре ставити на «аватар» фотографії інших людей без їх дозволу.

4. Поясніть дитині, що при спілкуванні на ресурсах, що вимагають реєстрації (у чатах, на форумах, через сервіси миттєвого обміну повідомленнями, в онлайн-іграх), краще не використовувати реальні ім'я та прізвище.

5. Поясніть дитині небезпеку зустрічі з незнайомими людьми з Інтернет. У мережі людина може представитися ким завгодно, тому на реальну зустріч з Інтернет-другом треба обов'язково ходити в супроводі дорослих.

6. Дитячий пізнавальний інтерес до теми сексуальних відносин між чоловіком і жінкою може активно експлуатуватися зловмисниками в Інтернеті. Постарайтеся самі поговорити з дитиною на цю тему. Поясніть їй, що нормальні відносини між людьми пов'язані з довірою, відповідальністю і турботою, але в Інтернеті тема кохання часто представляється в неправильній, вульгарній формі.

7. Якщо дитина бажає познайомитися з новим Інтернет-товаришем слід наполягти на супроводі дитини на цю зустріч

8. Проговорите з дитиною ситуацію і уважно вислухайте її. З'ясуйте у дитини всю можливу інформацію

9. Збережіть всі свідоцтва листування і контактів незнайомця з дитиною (скріншоти екрану, електронні листи, фотографії тощо).

10. При виявленні ознак замаху на злочин слід негайно повідомити про це в правоохоронні органи.

1.3.6. Негативний контент в мережі

До контентних ризиків відносяться матеріали (тексти, картинки, аудіо, відеофайли, посилання на сторонні ресурси), що містять протизаконну, неетичну і шкідливу інформацію. У першу чергу, з таким контентом можна зіткнутися на сайтах соціальних мереж, в блогах, на торрентах. Але сьогодні практично весь Інтернет - це віртуальний простір ризику.

Протизаконний контент – поширення наркотичних речовин через Інтернет, порнографічні матеріали за участю неповнолітніх, заклики до розпалювання національної ворожнечі і екстремістських дій.

Шкідливий (небезпечний) контент – контент, здатний завдати прямої шкоди психічному і фізичному здоров'ю особи.

Неетичний контент – контент, який не заборонено до поширення, але може містити інформацію, здатну образити користувачів. Такий контент може поширюватися обмежено (наприклад, «тільки для дорослих»). Особливо небезпечні сайти, на яких обговорюються способи заподіяння болю і шкоди, способи надмірного схуднення, способи самогубства, сайти, присвячені наркотикам, сайти, на яких розміщені статті, що пропагують насильство, спрямовані проти окремих груп чи осіб. Зіткнення з контентними ризиками може мати негативні наслідки для емоційної сфери, психологічного розвитку, соціалізації, а також фізичного здоров'я дітей підлітків або навіть дорослих осіб.

Основні правила мінімізації контентних ризиків

1. Використовуйте спеціальні технічні засоби, щоб обмежувати доступ дитини до негативної інформації – програми батьківського контролю і контентної фільтрації, налаштування безпечного пошуку. Часто пакет функцій батьківського контролю вже є у стандартній антивірусній програмі.

2. Програми батьківського контролю дозволяють: встановити заборону на відвідування сайтів різного негативного змісту, сайтів онлайн-знайомств, сайтів з шкідливим змістом; обмежити час доступу дитини до Інтернету; робити моніторинг листування в соціальних мережах і онлайн мессенджерах (чатах); блокувати сумнівні пошукові запити в пошукових системах; блокувати банери; а також

3. Ваш обліковий запис має мати надійний пароль і володіти правами адміністратора, щоб дитина не могла міняти встановлені вами настройки та програми.

4. Поясніть дітям, що далеко не все, що вони можуть прочитати або побачити в Інтернет – правда. Необхідно перевіряти інформацію, побачену в мережі. Для цього існують певні правила перевірки достовірності інформації. Ознаки надійного сайту, інформацією якого можна довіряти, включають: авторство сайту, контактні дані авторів, джерела інформації, акуратність подання інформації, мета створення сайту, актуальність даних. Розкажіть про ці правила вашим дітям та знайомим.

1.3.7. Безпека online покупок

Споживчі ризики – зловживання в Інтернеті правами споживача. Включають в себе: ризик придбання товару низької якості, різні підробки, контрафактної і фальсифікованої продукції, втрата грошових коштів без придбання товару або послуги, викрадення персональної інформації з метою кібершахрайства.

Основні правила online покупок

Перед тим, як зробити покупку в Інтернет магазині (online покупку) потрібно дотримуватися певних правил:

1. Здійснюйте покупки в великих Інтернет-магазинах, які добре зарекомендували себе на ринку.

2. Уважно читайте умови надання послуг, а також всі документи, одержувані при оформленні замовлення, наприклад, бланк замовлення, товарні накладні, рахунку і т. д.

3. Перевірте реквізити продавця, особливо якщо магазин не викликає довіри.

4. Запросіть підтвердження законності торговельної діяльності, переконайся, що представлений знак якості або сертифікат є справжніми.

5. Не довіряйте магазину тільки тому, що у його сайту красивий дизайн.

6. Читайте відгуки покупців про магазин, розміщені на сторонніх сайтах. Хоча виключити ймовірність того, що ці відгуки замовні, все одно не можна.

7. Порівнюйте ціни в різних Інтернет-магазинах за допомогою спеціальних сервісів.

8. Уточніть по телефону кінцеву вартість товару і його доставки, умови виконання замовлення, можливість отримання касового чека. Оцінить рівень культури спілкування продавця.

9. Не відправляйте про себе занадто багато інформації при здійсненні Інтернет-покупок: дані рахунків, паролі, домашні адреси і телефони. Пам'ятайте, що ніколи адміністратор чи модератор сайту не потребують повні дані вашого рахунку, паролі та пін-коди. Якщо хтось запитує подібні дані, будьте пильні – швидше за все, це шахраї.

10. Встановіть на свої комп'ютери антивірус або персональний брандмауер. Подібні додатки спостерігають за трафіком і можуть запобігти крадіжці конфіденційних даних або інші подібні дії.

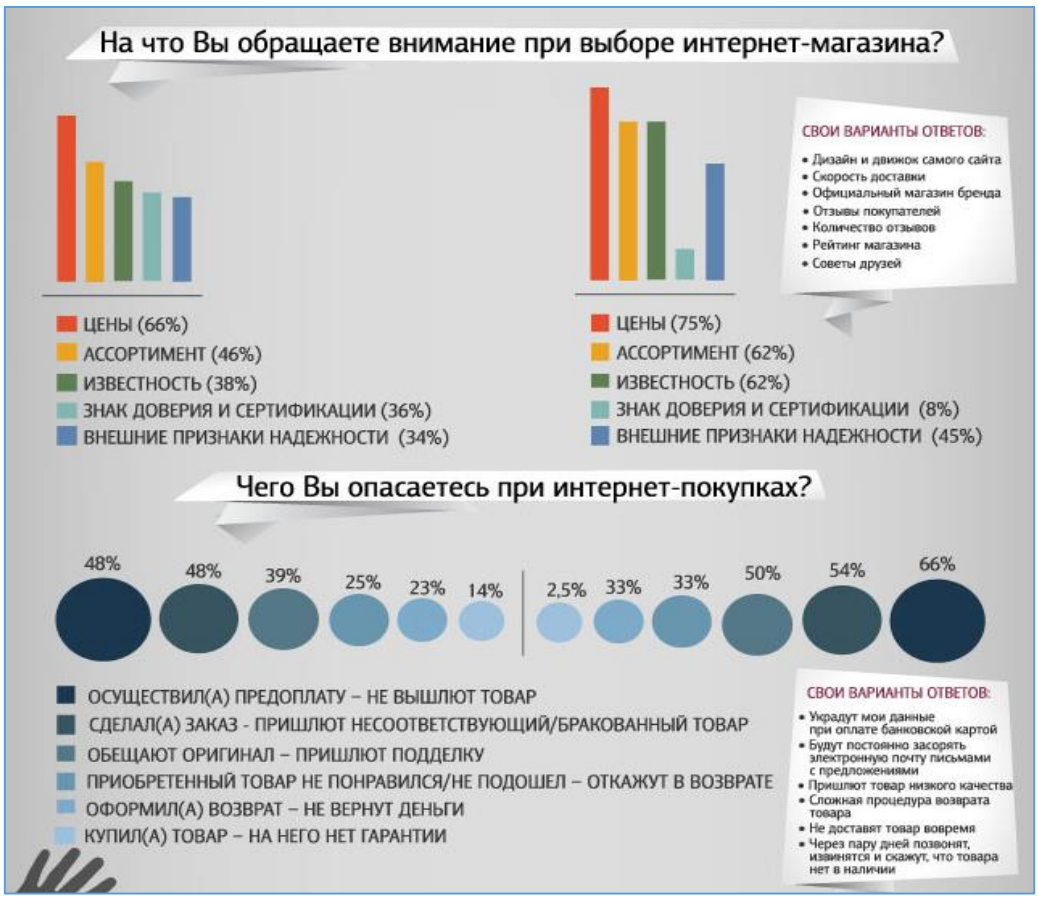


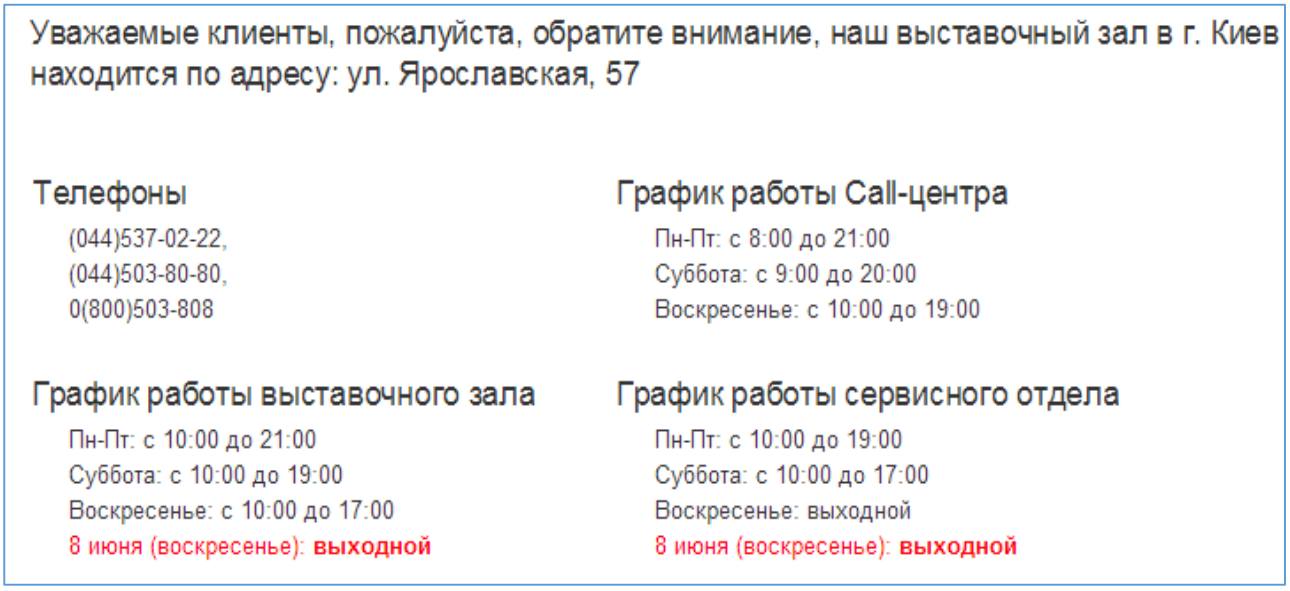
График работы call-центра приема и обработки заказов:

Понедельник-Пятница: с 8.00 до 21.00
Суббота: с 9.00 до 20.00
Воскресенье: с 9.00 до 19.00

По телефонам:

Отдел обработки заказов: (многоканальные линии)	(044) **323-03-34**, (057) **700-93-00** (067) **626-23-99**, (067) **219-99-96** **0 800 505-333** (бесплатно со стационарных телефонов Украины)
Корпоративный отдел: (Оформление заказов по безналичному расчёту)	(044) **323-06-11**, (067) **579-50-11**
Сервисный центр:	(044) **323-06-13**
Бухгалтерия:	(057) **700-93-05** (факс)

Приклад контактів крупного Інтернет магазину з гарною репутацією



Уважаемые клиенты, пожалуйста, обратите внимание, наш выставочный зал в г. Киев находится по адресу: ул. Ярославская, 57

Телефоны

(044)537-02-22,
(044)503-80-80,
0(800)503-808

График работы Call-центра

Пн-Пт: с 8:00 до 21:00
Суббота: с 9:00 до 20:00
Воскресенье: с 10:00 до 19:00

График работы выставочного зала

Пн-Пт: с 10:00 до 21:00
Суббота: с 10:00 до 19:00
Воскресенье: с 10:00 до 17:00
8 июня (воскресенье): **выходной**

График работы сервисного отдела

Пн-Пт: с 10:00 до 19:00
Суббота: с 10:00 до 17:00
Воскресенье: выходной
8 июня (воскресенье): **выходной**

Приклад контактів крупного Інтернет магазину з гарною репутацією

Наши контакты

Контакты интернет магазина

Получить квалифицированную консультацию, сделать заказ, согласовать время и место доставки вы можете по телефонам:

☎ (098)215-06-50

☎ (050)169-59-78

☎ (093)923-29-05

Жалобы и предложения оставляйте тут ✎:

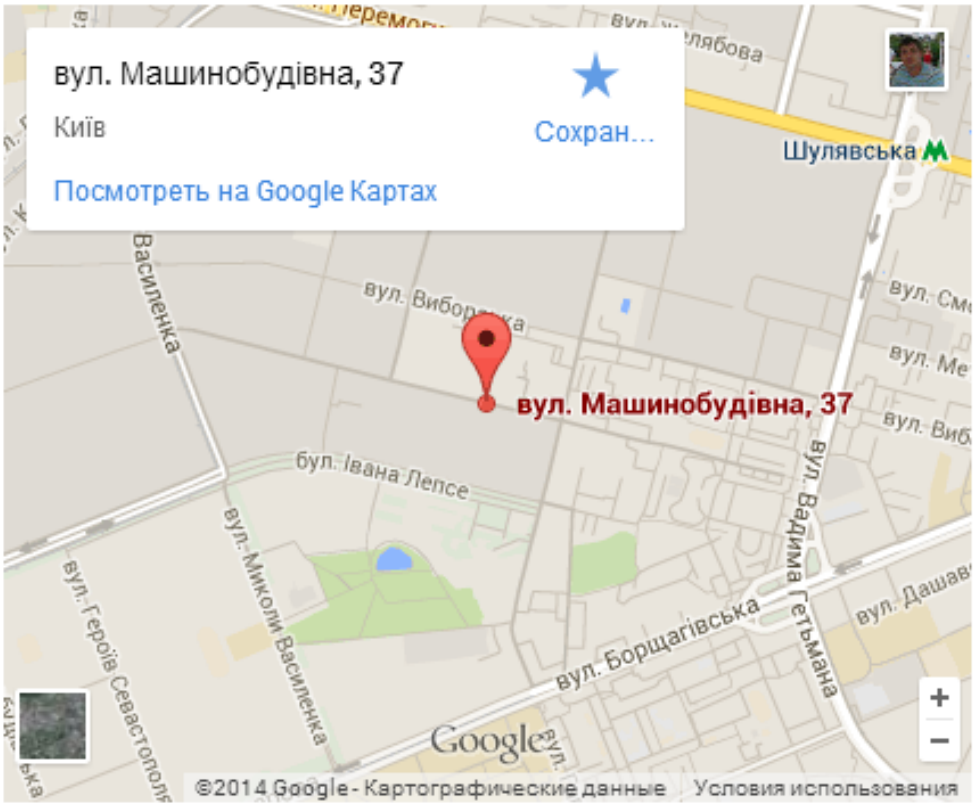
✉ shop@3da.com.ua

Прием телефонных звонков осуществляется Пт.-Сб. с 09:00 до 20:00

Приклад контактів Інтернет магазину, що можуть викликати сумнів в його репутації

Call-центр: +38(044)360-70-10

E-mail: sales@vipnokia.com.ua



Приклад контактів Інтернет магазину, що можуть викликати сумнів в його репутації

1.3.8. Безпека Інтернет банкінгу

За твердженнями експертів, основна і найголовніша загроза, яка турбує будь-якого користувача Інтернет-банкінгу – це ризик шахрайського злому і несанкціонованого доступу до коштів на рахунку. А тому банки намагаються використовувати різні системи і механізми, покликані якщо не гарантувати, то, принаймні, підвищити безпеку використання онлайн-банкінгу.

1. **Шифрування даних.** На сьогодні вже всіма або майже всіма банками, що надають послугу Інтернет-банкінгу, застосовується SSL-шифрування даних, переданих від комп'ютера користувача в систему банку і назад. Цей захід безпеки дозволяє виключити поширений раніше вид шахрайства «man in the middle», коли дані про платіж перехоплюються на етапі, коли вони відправлені від клієнта, але ще не дійшли в банк.

2. **Одноразові паролі, одержувані в банкоматі.** При такій системі захисту, крім звичайного логіна і пароля, для входу в систему і підтвердження операцій користувач повинен ввести одноразовий пароль, список яких він може отримати в банкоматі свого банку.

3. **Одноразові SMS-паролі.** Цей спосіб автентифікації користувача в системі Інтернет-банкінгу є чи не найпоширенішим у пропозиціях українських банків. При такій системі кожна операція, яку ви здійснюєте за допомогою онлайн-банкінгу, повинна бути підтверджена одноразовим паролем, який ви отримаєте в SMS-повідомленні на ваш мобільний телефон. При цьому ваш мобільний номер повинен бути «прив'язаний» до номера рахунку.

Така система має ряд переваг. По-перше, вона досить проста у використанні – вам не потрібно спеціальне обладнання, а процедура підтвердження операції займає всього пару хвилин. По-друге, вона дозволяє убезпечити ваш обліковий запис від використання зловмисниками - навіть якщо шахраям стане відомий ваш логін і пароль для входу в систему, вони не отримають доступ до ваших грошей, а ви дізнаєтеся про спробу провести несанкціоновану операцію з SMS-повідомлення. Крім цього, вам не потрібно зберігати список одноразових паролів, а значить, ви не зможете його втратити, і у вас його не вкрадуть.

На цьому переваги системи закінчуються. Дійсно, зловмисникам досить складно заволодіти одноразовим паролем, чинним протягом короткого часу. Якщо тільки вони не заволоділи вашим мобільним телефоном. І зовсім марною система буде в тому випадку, якщо ви користуєтеся Інтернет-банкінгом з

мобільного телефону і зберігаєте паролі в браузері. Тоді, вкравши у вас телефон, шахрай отримає ваш рахунок в повне розпорядження.

4. **Електронний цифровий підпис (ЕЦП).** Цей механізм частіше використовується при обслуговуванні банками компаній, але іноді його пропонують і індивідуальним клієнтам. Плюс ЕЦП в тому, що вона дозволяє однозначно ідентифікувати користувача. Недолік же полягає в тому, що ЕЦП також може бути вразлива для шахраїв. Зловмисники можуть дістатися до ключа від вашої цифрового підпису, заразивши ваш комп'ютер шкідливим програмним забезпеченням. Існують «троянці», що вміють знаходити і красти на зараженому комп'ютері автентифікаційні дані (ідентифікатори, паролі і навіть ключі ЕЦП) користувачів для доступу до різних сервісів (у тому числі і серверам віддаленого обслуговування клієнтів банків).

5. **Зовнішні електронні пристрої.** Деякі банки пропонують користувачам онлайн-банкінгу придбати (або взяти в оренду) спеціальний пристрій – генератор одноразових паролів. Генератор підключається до комп’ютера через usb-порт і не вимагає спеціального програмного забезпечення. Інші установи пропонують використовувати зовнішній електронний ключ, який генерується при першому підключенні до системи Інтернет-банкінгу, записується на зовнішній носій і потім використовується при проведенні операцій в системі. Такі системи, по суті, є спрощеною версією ЕЦП. Серед недоліків їх можна виділити те, що ви не зможете отримати доступ до свого рахунку, не маючи під рукою «ключа», а завжди носити його з собою може бути не дуже зручно і безпечно.

Які додаткові заходи застосовують банки для забезпечення безпечного користування Інтернет-банкінгом?

– обмеження використання особистого сертифікату - система деяких банків дозволяє використовувати електронний ключ (електронний сертифікат) тільки на тому комп'ютері, на якому він був згенерований. Таким чином, здійснювати платежі через Інтернет-банкінг ви зможете тільки зі свого особистого комп'ютера (хоча переглядати виписки по рахунку можна і на інших пристроях);

– віртуальна клавіатура – призначена для того, щоб шахраї не могли «рахувати» ваші реєстраційні дані при введенні їх із звичайної клавіатури за допомогою комп'ютерних вірусів («троянів»);

– обмеження тривалості сесії – у разі неактивності користувача, сесія в системі Інтернет-банкінгу через певний час (зазвичай 10-15 хвилин) буде закрита. Після цього для відновлення роботи потрібно заново пройти аутентифікацію;

– історія підключень – за допомогою цієї функції користувач Інтернет-банкінгу дізнається, якщо хтось крім нього підключався до системи, а також зможе відстежити всі несанкціоновані операції, якщо вони були зроблені.

Як не потрапити в небезпеку при використання систем Інтернет-банкінгу?

а) Якщо для підтвердження Ваших фінансових операцій через Інтернет ви використовуєте ЕЦП, не забувайте користуватися антивірусними програмами і регулярно перевіряти ваш комп'ютер на предмет зараження комп'ютерними вірусами. Також експерти не радять залишати ключ ЕЦП підключеним до комп'ютера, якщо ви його не використовуєте.

б) Якщо ваш банк використовує автентифікацію користувача по SMS, постарайтеся дотримуватися таких правил:

– не користуйтеся Інтернет-банкінгом з мобільного телефону;

– видаляйте пароль від облікового запису в браузері;

– у разі втрати або крадіжки мобільного телефону – негайно зверніться в банк з проханням заблокувати ваш обліковий запис Інтернет-банкінгу.

в) Щоб скористатися всіма перевагами захищеної передачі даних, слід дотримуватися елементарних заходів безпеки в Інтернеті – не реагувати на підозрілі повідомлення (отримані нібито від вашого банку) і не переходити з невідомих посиланнях.

г) Крім того потрібно:

– використовувати антивірусне програмне забезпечення і міжмережеві екрани (файерволи), відомих виробників;

– обмежувати доступ до комп'ютерів, з яких ведеться робота з системою Інтернет-банкінг, стороннім особам;

– нікому не повідомляти свій пароль. Співробітники банку ніколи, ні за яких обставин не запитують паролі користувачів;

– не зберігати ключ електронно-цифрового підпису на чужих комп'ютерах;

– уникати проведення платежів або зміни паролів з комп'ютерів, до яких має доступ безліч людей (комп'ютери в Інтернет-клубах, залах очікування на вокзалах, аеропортах і т.п.), на них може бути встановлено шкідливе програмне забезпечення.

1.4. КІБЕРЗЛОЧИНИ ТА ДОВІД БОРОТЬБИ З НИМИ ЗА КОРДОНОМ

1.4.1. Поняття «кіберзлочинність»?

Звертаємо увагу, що незважаючи на те, що поняття «*кіберзлочинність»* і пов’язана з ним термінологія використовується досить широко, офіційного, закріпленого в міжнародних документах та/або національному законодавстві визначення кіберзлочинності досі не існує. Навіть у Конвенції про кіберзлочинність 2001 року і додаткових протоколах до неї використовуються поняття «комп'ютерна система», «комп'ютерні дані» та передбачається встановлення відповідальності за «правопорушення проти конфіденційності, цілісності та доступності *комп'ютерних* даних і систем; за навмисне перехоплення технічними засобами, без права на це передач *комп'ютерних* даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування *комп'ютерної* інформації без права на це; навмисне серйозне перешкоджання функціонуванню *комп'ютерної* системи» тощо.

Згідно рекомендаціям експертів ООН, термін «кіберзлочинність» охоплює будь-який злочин, який може здійснюватися за допомогою комп’ютерної системи або мережі, в рамках комп’ютерної системи або мережі, проти комп’ютерної системи або мережі.

Інакше кажучи, до кіберзлочинів відносяться такі суспільно небезпечні діяння, які здійснюються в кіберпросторі за допомогою або з використанням комп’ютерних систем або комп’ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп’ютерних систем або мереж і проти комп’ютерних систем, комп’ютерних мереж і комп’ютерних даних.

1.4.2. Підрозділи, що здійснюють боротьбу із кіберзлочинами?

У США створено такі відомства, як Electronic Crimes Task Forces (ECTF), US Cyber Command (військовий підрозділ, який здійснює свою діяльність у кіберпросторі), United States Computer Emergency Readiness Team (національний відділ кіберзахисту Департаменту внутрішньої безпеки США), Computer Crime and Intellectual Property Section (відділ комп'ютерної злочинності і інтелектуальної власності Міністерства Юстиції США).

У Великій Британії боротьбою з кіберзлочинністю займається відділ по боротьбі з кіберзлочинами (National Cyber Crime Unit), що входить до складу Агентства по боротьбі зі злочинністю.

У ФРН основну діяльність щодо боротьби з кіберзлочинністю здійснює Федеральна кримінальна поліція, а точніше департамент по боротьбі з тяжкими злочинами та організованою злочинністю (Abteilung «Schwere und Organisierte Kriminalität»" (SO).

У Франції 1 липня 2008 р. шляхом об'єднання двох спецслужб Центрального директорату загальної розвідки (RG) і Директорату стеження за територіями (DST) створено Головне управління внутрішньої розвідки Direction centrale du Renseignement interieur, DCRI. - однією з функцій даного управління є боротьба з кіберзлочинністю.

1 січня 2009 в складі Бюро кримінальної поліції Литви було створено Управління з розслідування злочинів в електронній середовищі. У складі Управління було створено два відділи: відділ з розслідування злочинів, відділ технічної підтримки. В Білорусі діє Управління з розкриття злочинів у сфері високих технологій (Управління К).

Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна організація безпеки - НАТО (Cooperative Cyber Defence Centre of Excellence). У 2008 році Спільний Центр передового досвіду з кіберзахисту в Таліні, Естонія, був акредитований як Центр передового досвіду НАТО. Він проводить дослідження та навчання у сфері кіберзахисту (7). У січні 2013 року в Гаазі, Нідерланди, почав роботу Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre).

1.4.3. Програмне забезпечення, що може допомогти виявити та розкрити злочини, які пов'язані з використанням комп'ютерної та мобільної техніки

Для відстеження активності в соціальних мережах у Росії розробили і використовують систему моніторингу соціальних мереж – спеціальні термінали **«Призма».**[9] Система «Призма» в реальному часі відслідковує 60 млн джерел. Вона показує динаміку позитивних і негативних відгуків в Інтернет на ту чи іншу подію, а також здатна будувати графіки атак ботів. При цьому відстеження тем моніторингу настроюються індивідуально.

Система аналізує інтерес до тих чи інших проблем і попереджає про можливі репутаційні ризики. Вона також дає можливість оцінювати реакцію в соціальних медіа на основні події та ініціативи відомства, регіону, керівника, допомагає відслідковувати факти корупції в рамках регіону чи відомства і миттєво реагувати на них

Крім того, за твердженнями розробників, «Призма» оперативно відстежує в соцмедіа активності, що призводять до зростання соціальної напруженості: нагнітання безладів, протестні настрої, екстремізм; обговорення рівня цін, проблеми ЖКГ, інфраструктури, медицини та ін. Система «Призма» може бути оперативно розгорнута впродовж декількох днів. Клієнтська частина рішення - брендований моноблок з встановленим програмним забезпеченням.

Програмний продукт **Elcomsoft iOS Forensic Toolkit**[10] являє собою спеціалізоване програмне забезпечення для криміналістичного дослідження пристроїв на основі Apple iOS. За допомогою програми можна «витягти» весь вміст пам'яті телефону, а це і листування, і комунікації в соціальних мережах, і навіть повна історія дій користувача, інформацією про точне місцезнаходження користувача, яка визначається датчиками GPS або обчислюється за силою сигналу найближчих сот. Більш того, за допомогою iOS Forensic Toolkit можна відновити оригінальний пароль користувача на включення телефону, що відкриває повний доступ до так званих секретів пристрою - інформації, що знаходиться в спеціальному зашифрованому сховище. Вся процедура вилучення

[9] Сайт розробника: http://www.mlg.ru/solutions/4executives/prizma
[10] Сайт розробника http://www.elcomsoft.ru/eift.html

і розшифровки інформації відбувається в режимі реального часу - криміналісту не потрібно очікувати, поки буде зламаний пароль від резервної копії даних.

Програмно-апаратний комплекс **«Мобільний криміналіст»**[11] компанії Oxygen здатний не тільки витягти інформацію з декількох тисяч моделей телефонів (на сьогоднішній день заявлена підтримка 6300 моделей), а й пропонує найпотужніший аналітичний функціонал. Одна з дійсно цікавих особливостей «Мобільного криміналіста» - можливість виявлення не тільки контактів конкретного користувача, але і взаємозв'язку між користувачами різних пристроїв. Досить витягти дані з телефонів, конфіскованих у групи зловмисників, і програма не тільки відновить активність всіх членів групи, збудувавши всі дії користувачів телефонів у вигляді хронологічної стрічки подій, але і сформує чіткий графік, на якому легко відстежити всі взаємодії та взаємозв'язку членів групи.

Припустимо, у нас є жорсткий диск, знятий з ПК підозрюваного, або навіть весь комп'ютер цілком. Що з цим можна зробити? Існує лінійка продуктів під назвою **Belkasoft Evidence Center**[12], яка призначена для збору доказів з жорстких дисків та образів пам’яті комп’ютерів. При розробці програми враховані всі вимоги до подібного класу продуктів: забезпечується збереження оригінального стану диска, а доступ до інформації відбувається безпосередньо, незважаючи на всі заборони файлової системи. При виявленні доказів слідчий отримує точну фізичну адресу, однозначно ідентифікує місце на диску, де зберігаються ці дані. Якщо виникне питання автентичності знайдених доказів – інформацію завжди можна перевірити ще раз будь-яким інструментом низькорівневого аналізу диску.

1.4.4. Деякі приклади протидії кіберзлочинам за кордоном?

У Великобританії особливу увагу правоохоронні органи звертають на боротьбу з розповсюдженням наркотичних речовин через мережу Інтернет. У п. 3.2.1 Методичних рекомендацій по боротьбі з вирощуванням коноплі та точками її збуту наголошується, що правоохоронці мають здійснювати періодичний пошук інформації про продаж наркотичних засобів у мережі. При цьому, у разі виявлення таких об’єктів підслідність з розслідування цих злочинів реалізується

[11] Сайт розробника http://www.oxygen-forensic.com/ru/
[12] Сайт розробника: http://ru.belkasoft.com/ru/bec/en/evidence_center.asp

за територіальним принципом, тобто розслідування проводить той правоохоронний орган, на території якого фізично розташовано виявлений об’єкт.

Законодавство Німеччини є досить жорстким щодо незаконних дій з використанням електронних інформаційних систем. Після гострих дебатів у 2008 році Конституційний суд ФРН своїм рішенням дозволив проведення таємних онлайн-обшуків персональних комп’ютерів підозрюваних у разі суворого дотримання низки умов. Згідно з § 20k Закону «Про федеральне управління кримінальної поліції» Федеральна кримінальна поліція може без відома підозрюваного, проникати за допомогою технічних засобів до інформаційно-технічних систем, що використовуються підозрюваним, та вилучати з них дані про нього, за умови наявності встановлених фактів того, що існує загроза:

– здоров’ю, життю або свободі особи;

– суспільним цінностями, які становлять основу стабільності держави або основу існування людей.

Під час використання спеціальних технічних засобів:

– до інформаційно-технічної системи вносяться тільки ті зміни, які потрібні для збирання даних;

– після закінчення заходу вносяться всі можливі технічні зміни, які автоматично повертають систему до вихідного стану.

Засоби, що використовуються, мають забезпечувати технічний захист від несанкціонованого використання. Скопійовані дані мають бути технічно захищені від змін, несанкціонованого використання та несанкціонованого ознайомлення.

Використання технічного засобу має бути запротокольоване із зазначенням:

– характеристик технічного засобу і часу його використання;

– технічних даних ідентифікації інформаційно-технічної системи, а також тих систем, в яких проводилися навіть незначні зміни;

– інформації, що дозволяє встановити місце розташування зібраних даних;

– відомостей про підрозділ, який проводить цей захід.

Указані заходи здійснюються на підставі судового ордеру. Ордер видається в письмовій формі. У ньому має бути вказано:

– якщо відомо, прізвище та адреса особи, стосовно якої проводиться захід;

– по змозі точна характеристика інформаційно-технічної системи, в якій має проводитися збирання даних;

- тип, межі та тривалість заходу із зазначенням часу його закінчення;
- головні причини проведення.

Ордер видається на строк, що не перевищує один місяць. У кожному окремому випадку продовження ордеру допускається на термін не більше трьох місяців, якщо умови, вказані в ордері (з урахуванням отриманих результатів), продовжують існувати. У разі відсутності підстав, за якими видано ордер, заходи, ним санкціоновані, негайно припиняються.

Правоохоронцями США з точки зору вчинення протиправної діяльності комп'ютер розглядається у трьох ракурсах. По-перше, він може виступати як знаряддя вчинення злочину з метою викрадення інформації або завдання шкоди цільовій системі. По-друге, комп'ютер може розглядатися як засіб вчинення злочину, наприклад, для електронного шахрайства. І, по-третє, комп'ютер розглядається як сховище для доказової інформації або контрабанди.

На цей час у ФБР розроблено спеціальні програми для порівняння зображень з метою виявлення в Інтернеті дитячої порнографії; програми для відстежування серверу, з якого було відправлено те або інше електронне повідомлення або розміщено WEB-сторінку; програми документування сесій чатів; програми для виявлення закодованих стеганографічних повідомлень тощо.

Також працівники ФБР часто проводять операції по боротьбі з дитячою порнографією, під час яких агенти відвідують спеціальні чати, форуми, тематичні сайти з дитячою порнографією, де виявляють потенційних злочинців та документують їх протиправну діяльність з метою притягнення до кримінальної відповідальності. Право на проведення особистого пошуку за допомогою кіберпростору (відвідування сайтів, форумів тощо) з метою виявлення та припинення злочинів закріплено в Інструкції Генерального прокурора «Про здійснення ФБР місцевих операцій.

Також працівники ФБР можуть видавати себе і за неповнолітніх, спілкуючись з педофілами. Проведення таких оперативних комбінацій шляхом використання кіберпростору у США має назву «онлайнові секретні операції» (online undercover operations). Строк проведення таких операцій встановлюється не більше 30 діб, але за необхідності його можна подовжити. Санкцію на їх проведення видає спеціальний агент, а за наявності певних обставин ця санкція погоджується зі Штаб-квартирою ФБР. Результати проведення такої операції фіксуються у відповідному звіті.

Під час проведення онлайнової секретної операції секретний співробітник зобов'язаний:

- робити точні записи всіх онлайнових комунікацій;
- уникати будь-якої незаконної діяльності;

– підтримувати онлайновий профіль (параметри користувача) по змозі в обмеженому вигляді, достатньому для досягнення мети операції;

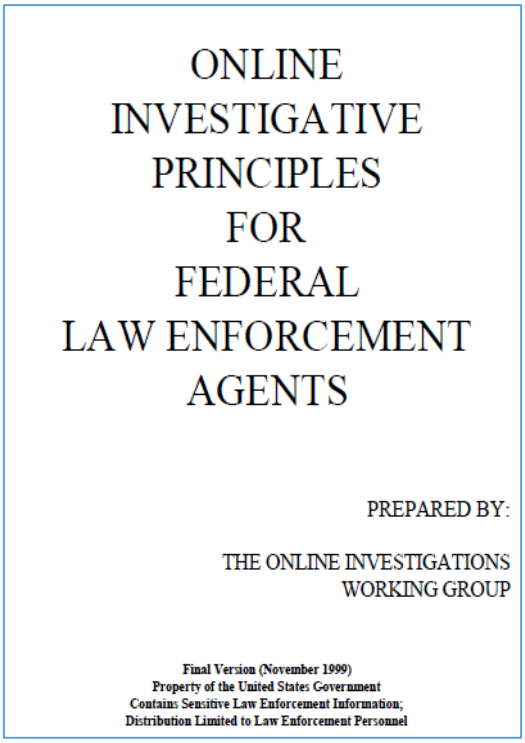
– уникати фізичного контакту з фігурантами;

– робити всі необхідні дії протягом періоду операції для захисту потенційних жертв та попередження серйозної кримінальної діяльності, якщо під час онлайнового контакту з'ясується, що існує реальна серйозна загроза третім особам, комерційним організаціям або урядовим об'єктам;

– припинити секретну діяльність, якщо протягом 30 діб буде ухвалено рішення про припинення секретної операції.

Базовим документом, який регламентує використання кіберпростору правоохоронними органами США, є «Правила онлайнових розслідувань для правоохоронних органів» 1999 р. (далі Правила онлайнових розслідувань). Правила онлайнових розслідувань були розроблені спеціальною міжвідомчою робочою групою, до якої входили представники майже всіх правоохоронних органів США. Задля розуміння агентами змісту цього документу в ньому наведено багато аналогій між кіберпростором (cyberspace) та реальним середовищем (physical world).

До 2004 р. Правила онлайнових розслідувань мали обмежений доступ і поширювалися лише у відповідних правоохоронних органах. Цим документом закріплюються основні правила, яких повинні дотримуватися правоохоронці під час виявлення, припинення та розкриття злочинів шляхом використання кіберпростору.


ONLINE
INVESTIGATIVE
PRINCIPLES
FOR
FEDERAL
LAW ENFORCEMENT
AGENTS

PREPARED BY:

THE ONLINE INVESTIGATIONS
WORKING GROUP

Final Version (November 1999)
Property of the United States Government
Contains Sensitive Law Enforcement Information;
Distribution Limited to Law Enforcement Personnel

Титульна сторінка зазначених рекомендації про проведення online розслідувань

1.5. РЕКОМЕНДАЦІЇ ЩОДО ДІЯЛЬНОСТІ ОВС ПО МІНІМІЗАЦІЇ ІНТЕРНЕТ-РИЗИКІВ

1. Завданням зазначених методичних було проаналізувати зміст найбільш поширених ризиків мережі Інтернет та узагальнити досвід щодо зменшення їх впливу на громадян з боку органів внутрішніх справ.

2. Мінімізація Інтернет-ризиків, в першу чергу, полягає у проведенні попереджувальної роботи з боку органів внутрішніх справ, що дозволяє проінформувати громадян про особливості Інтернет-ризиків, надання рекомендацій щодо їх уникнення, розробки адекватного механізму взаємодії органів та підрозділів внутрішніх справ з державними органами, громадськими організаціями, окремими громадянами щодо їх попередження.

3. Важливим напрямом вважаємо подальшу розбудову сайту Управління боротьби з кіберзлочинністю МВС України: http://cybercrime.gov.ua/ua:

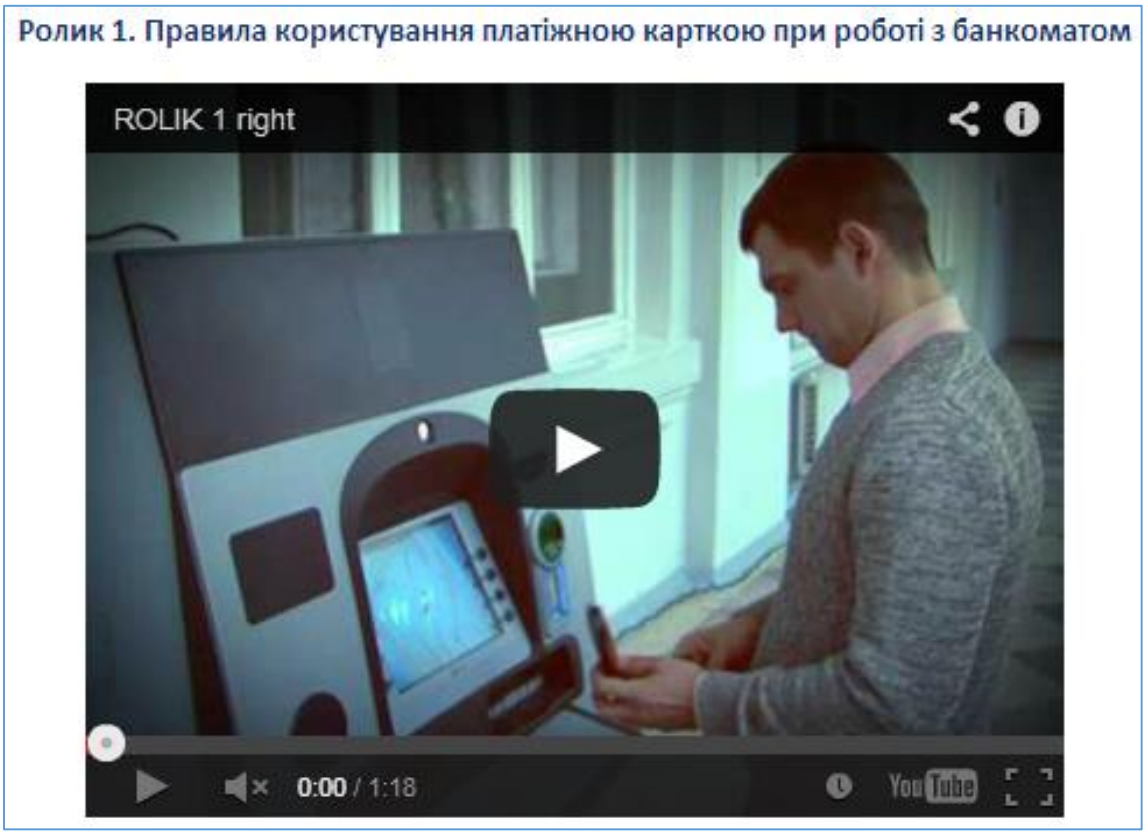
– доцільним є продовження його змістовного наповнення щодо класифікації найбільш поширених Інтернет-загроз, засоби протидії їм з боку органів держави, громадських організацій та громадян. **Для цього рекомендуємо використовувати зміст цієї роботи, як основу.**

– на сайті варто навести приклади найбільш розповсюджених загроз, приклади Інтернет-шахрайств, фото, відео, інший матеріал щодо небезпек в мережі Інтернет. Наприклад корисними можуть бути матеріали спеціалізованого сайту http://anticyber.com.ua. Досить цікава підбірка начальних фільмів та матеріалів міститься на каналі GroupIB: https://www.youtube.com/channel/UCHl7R4F66A_B0S-WH42ZD6Q, на сайті незалежної асоціації банків України: http://www.nabu.com.ua/ukr/press_centr/media/video/?id=533, у Центрі безпеки Google: http://www.google.ru/intl/ru/safetycenter;

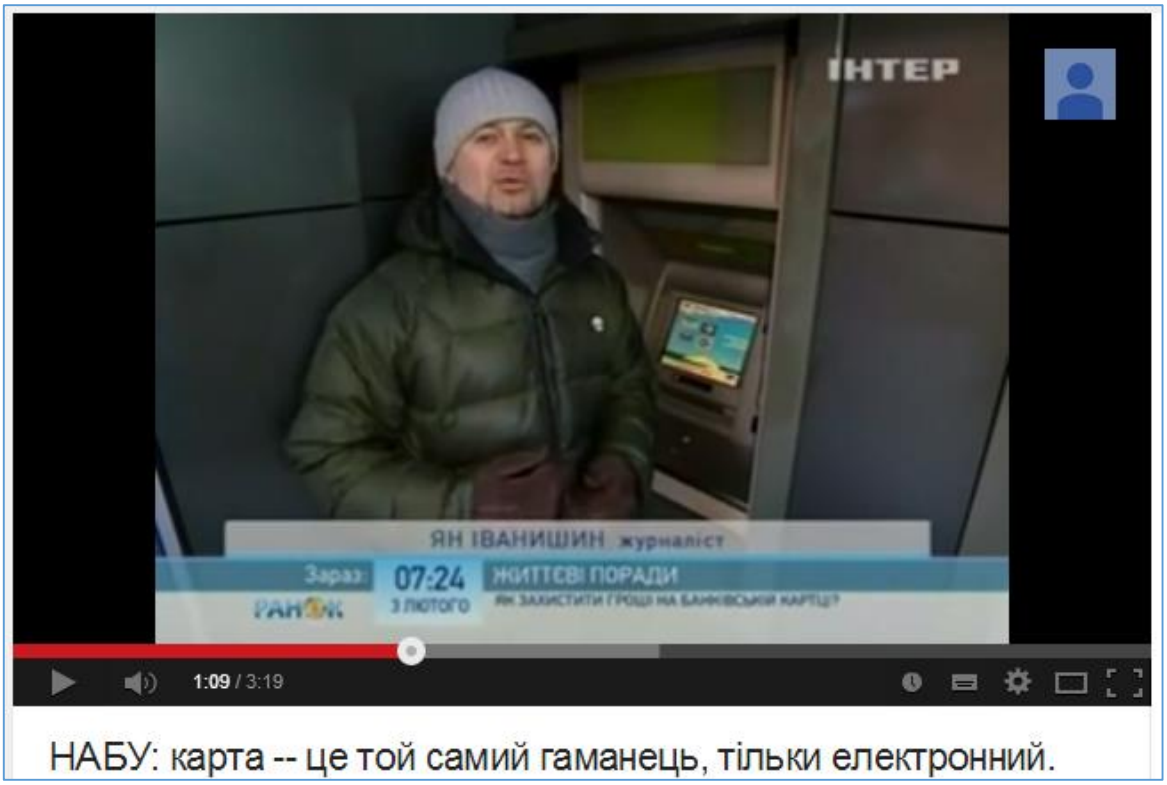
– актуальним є публікація на сайті наукових статей та міжнародних документів, присвячених боротьбі із кіберзлочинністю, які можуть бути основою для нормотворчої роботи та наукових досліджень в цій сфері. Наприклад, одним з останніх міжнародних документів є перекладене російською мовою «Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора», резюме якого було прийнято у лютому 2013 року в Відні.[13]

[13] Адреса документу: http://goo.gl/TPcNqY

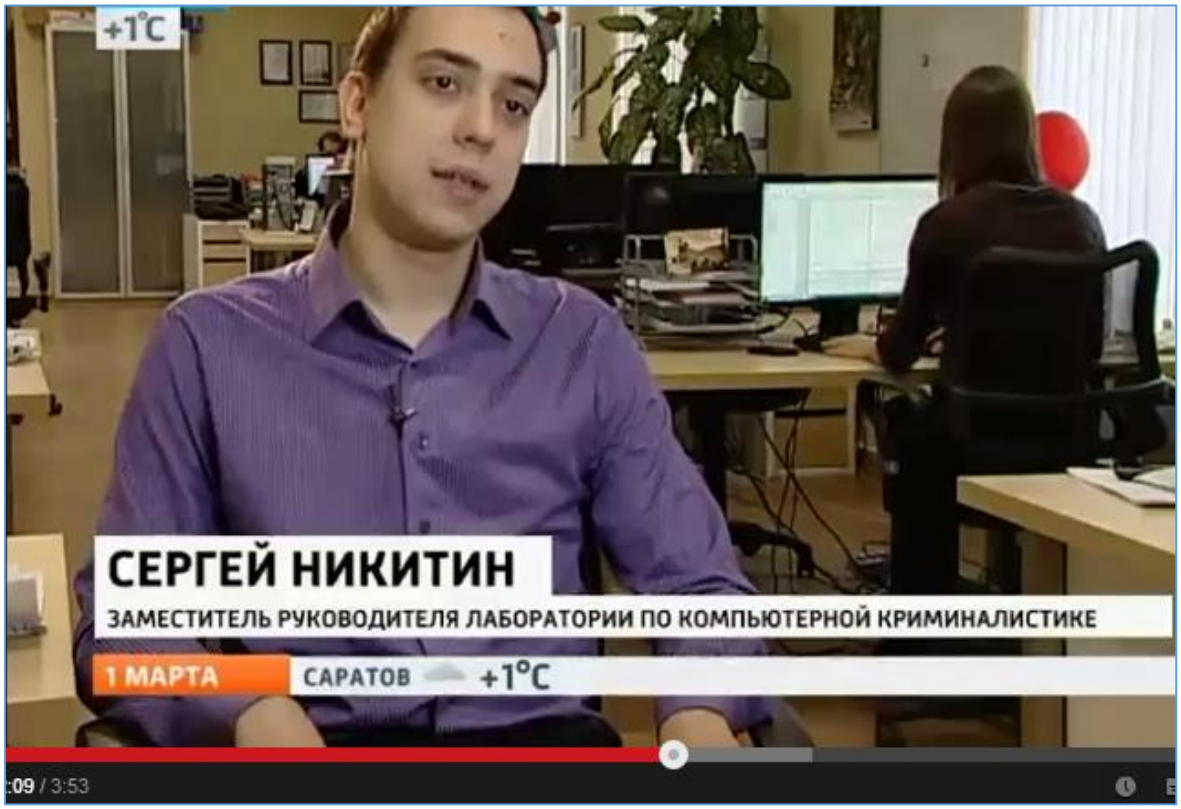
Довід роботи незалежної асоціації банків України щодо безпеки онлайн платежів



Навчальне відео незалежної асоціації банків України щодо користування платіжними картками



Незалежне розслідування журналістів каналу «Інтер» щодо шахрайства в Інтернет



Відео компанії groupIB[14] щодо розповсюджених кіберризиків

14 Group-IB - провідна міжнародна компанія з запобігання та розслідування кіберзлочинів і шахрайств з використанням високих технологій.

4. Зважаючи на те, що проблематика правопорушень, які пов’язані з Інтернет-ризиками входить до сфери діяльності, як Управління боротьби з кіберзлочинністю МВС України так і Управління кримінальної міліції у справах дітей, то можливе співробітництво вказаних підрозділів в профілактичній роботі по мінімізації Інтернет-ризиків, особливо в підлітковому середовищі.

5. Перспективним напрямом діяльності органів внутрішніх справ у мінімізації Інтернет-ризиків, є завчасне формування кадрового резерву та популяризації безпечного Інтернету серед молоді. В цьому напрямі доцільно:

– запровадити практику створення навчальних фільмів про найбільш розповсюджені ризики мережі Інтернет;

– запровадити цикл передач для зацікавлених верств населення, в тому числі й молоді, про ризики мережі Інтернет;

– здійснювати моніторинг діяльності навчальних закладів, що готують фахівців у сфері комп’ютерних технологій, з метою проведення профорієнтаційної роботи та запрошення найбільш талановитих випускників ВНЗ на роботу до підрозділів ОВС, які здійснюють боротьбу з кіберзлочинами. Крім того, можливе проведення конкурсів на кращі розробки в сфері комп’ютерної безпеки серед студентів ВНЗ, в тому числі й серед курсантів ВНЗ МВС України;

– запровадити у середніх навчальних закладах проведення лекційних занять з учнями щодо небезпек всесвітньої мережі Інтернет, конкурсів малюнків тощо, можлива робота і з батьками школярів та педагогами. Наприклад, можна розміщувати в мережі пам’ятки, на кшталт такої, що представлена у **Додатку** А.

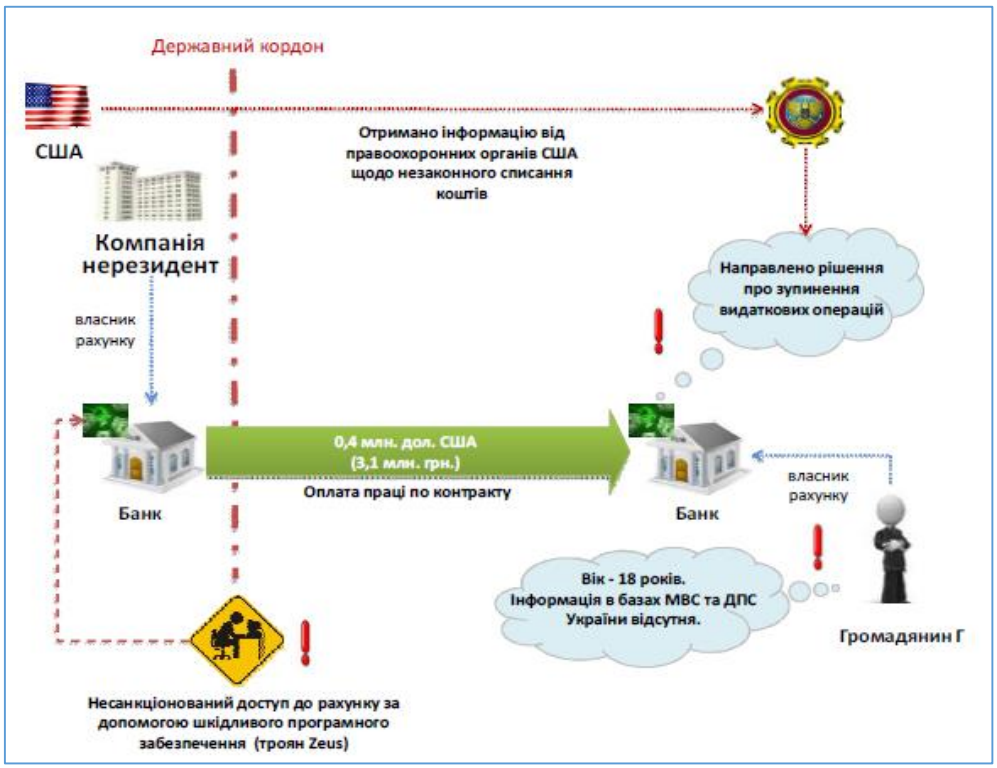
6. Велику роль в мінімізації Інтернет-ризиків, має відігравати цілеспрямована робота провайдерів та правоохоронних органів щодо блокування в українському сегменті Інтернет ресурсів, які містять інформацію порнографічного характеру, пропагують насилля, жорстокість, призивають до міжнаціональної ворожнечі. Так, сьогодні з багатьма національними провайдерами проводяться постійні переговори щодо обмеження доступу до негативного контенту. Але, нажаль, діяльність ОВС обмежена рамками України. Інтернет, як відомо, не має меж, і сервери з небезпечним контентом можуть бути розташованими в іншій країні.

7. Взаємодія органів внутрішніх справ з фінансовими установами – наприклад приватними банками та Національним банком України, Державною службою фінансового моніторингу України. Результатом такого співробітництва може стати проведення спільних конференцій, симпозіумів, обміну досвідом щодо розслідування злочинів пов’язаних із Інтернет ризиками, спільне виготовлення агітаційних матеріалів, матеріалів щодо найбільш розповсюджених схем шахрайства в мережі Інтернет, посібників тощо.

Прикладом такої продукції є методичні матеріали Департаменту фінансових розслідувань Державної служби фінансового моніторингу України «Кіберзлочинність та відмивання коштів».

Крім того, протягом останнього року незалежна асоціація банків України представила концепцію протидії кіберзлочинності в банківській сфері. Концепція передбачає створення ефективної загальнодержавної системи протидії кіберзлочинності у банківській сфері та створення платформи для комунікації між банками, регуляторами, МВС України та іншими учасниками. Концепція, зокрема передбачає створення єдиної інформаційної бази банків з метою обміну антишахрайською інформацією.

Основні принципи роботи бази: доступ всіх банків до інформації; знеособленість інформації в системі; НБУ співпрацює з МВС та іншими держструктурами у сфері дієвих превентивних заходів, здійснення яких не суперечить законодавству України, в т.ч. порядку/форми обміну інформацією превентивного характеру; захист інформації системи на державному рівні. Отже МВС України має приймати активну участь у реалізації цієї Концепції.



Фрагмент матеріалів ДМФМУ «Кіберзлочинність та відмивання коштів»

8. В подальшій перспективі логічним кроком є заключення договорів з боку МВС про співпрацю з представництвами найбільших комп'ютерних компаній з метою спільної роботи та обміну досвідом у боротьбі з кіберризиками. Наприклад, в США та Японії за участю Microsoft, Xerox, Google,

НР були створені центри реагування на кіберзлочини. Такий же центр існує в Китаї. Робота центрів зводиться до моніторингу кіберзагроз та розробці ефективних методів протидії.

9. Рекомендуємо Управлінню боротьби з кіберзлочинами та Управлінню в справах дітей МВС України за можливої підтримки навчальних закладів системи МВС, розробити агітаційні матеріали про ризики мережі Інтернет та засоби їх запобігання. Прикладом таких матеріалів може бути Інфографіка про безпеку online покупок (Додаток Б). Для розробки матеріалів можна залучати представників підрозділів ОВС, які здійснюють дослідження цієї тематики, наприклад, Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах Харківського національного університету внутрішніх справ (http://cybercop.in.ua).

10. Потрібно включити до системи службової підготовки, програм підвищення кваліфікації особового складу питання мінімізації Інтернет-ризиків працівниками ОВС, як щодо громадян, так і в самій інформаційній системі ОВС. Адже, службові та особисті комп’ютери працівників ОВС також можуть бути під загрозою спаму, фішингових повідомлень, хакерських атак, вірусів тощо.

11. Актуальним, на наш погляд, є включення до програм підвищення кваліфікації працівників ОВС питань пов’язаних із боротьбою з правопорушеннями, що пов’язані з Інтернет-ризиками (Додаток В).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про кіберзлочинність [Електронний ресурс]: Міжнародний документ від 23.11.2001 р. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

2. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р., № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71

3. Литовченко І.В., Максименко С.Д., Болтівець С.І. Діти в Інтернеті: як навчити безпеці у віртуальному світі / І.В. Литовченко, С.Д. Максименко, С.І. Болтівець – К.: Видавництво: ТОВ «Видавничий будинок «Аванпост-Прим», 2010. - 48 с. (Посібник для батьків).

4. Безпека банківської діяльності: монографія / Казакова Н.Ф., Панфілов В.І., Скачек Л.М., Скопа О.О., Хорошко В.О.; за ред. проф. Хорошко В. О. – К. : ПВП «Задруга», 2013. – 282 с.

5. Гавловський В.Д. Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів / В.Д. Галовський // Питання інформаційної безпеки. – 2012. -№ 2 (28). – С. 271-281

6. Йона О.О., Казакова Н.Ф. Світові тенденції боротьби з кіберзлочинністю / О.О. Йона, Н.Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. - № 15 (204). - Ч.1. – С. 59-61

7. АНТИ-CyberMOBBING (моббинг, боссинг, буллинг) Защитим от моббинга! [Електронний ресурс]: Громадська ініціатива у соціальній мережі ВКонтакте. – Режим доступу: http://vk.com/anticybermobbing

8. Валевский В. Интернет-троллинг и кибербуллинг. Что это? [Електронний ресурс] / В. Валевский. – Режим доступу: http://www.stihi.ru/2012/04/20/10137

9. Ваш ребенок и социальные сети: простые правила [Електронний ресурс]: Офіційний блог компанії «Лабораторія Касперського». – Режим доступу: http://blog.kaspersky.ru/simple-rules-kids-social/

10. Глобальная сеть: правила пользования: Рекомендации для родителей [Електронний ресурс]. – Режим доступу: http://detionline.com/assets/files/journal/8/pract_8.pdf

11. Интернет-преступники: помощь в уменьшении риска [Електронний ресурс]: Центр безпеки компанії Microsoft. – Режим доступу: http://www.microsoft.com/ru-ru/security/family-safety/predators.aspx

12. Зельцер Ленни Онлайн шоппинг: техника безопасности // OUCH!. - Ноябрь 2013 (OUCH! – ежемесячный журнал по информационной

безопасности). – Режим доступу: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201311_ru.pdf

13. Как защититься от фишинг-атак и других действий мошенников [Електронний ресурс]: Офіційний сайт компанії Microsoft. – Режим доступу: http://www.microsoft.com/ru-ru/security/online-privacy/phishing-scams.aspx

14. Киберпреступность в США [Електронний ресурс]. – Режим доступу: http://goo.gl/vmB0OH

15. Кривошеев И. Мошенничество в Интернете [Електронний ресурс]. – Режим доступу: http://www.neumeka.ru/moshennichestvo_v_internete.html

16. Найденова Л. Кибер-буллинг: опасное виртуальное «быкование» [Електронний ресурс] / Л. Найденова. – Режим доступу: http://psyfactor.org/lib/cyber-bullying.htm

17. Обманщики в соціальних мережах [Електронний ресурс]: Офіційний сайт незалежної асоціації банків в Україні . – Режим доступу: http://anticyber.com.ua/article_detail.php?id=244

18. Основы детской безопасности [Електронний ресурс]: Центр безпеки компанії Google. – Режим доступу: https://www.google.ru/safetycenter/families/start

19. Орлов О.В., Онищенко Ю.М. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю [Електронний ресурс] / О.В. Орлов, Ю.М. Онищенко // Теорія та практика державного управління. – 2013. - № 3(42). – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/tpdu/2013-3/doc/1/01.pdf

20. Поведение детей в Интернете и on-line риски сексуальной эксплуатации детей в Кыргызстане [Електронний ресурс]: Центр изучения общественного мнения и прогнозирования «Эл-Пикир». – Режим доступу: http://elpikir.org/news/36-rezultaty-issledovaniya-povedenie-detey-v-internete-i-online-riski-seksualnoy-ekspluatacii-detey-v-kyrgyzstane.html

21. Проект Незалежної асоціації банків України (НАБУ) «Протидія» кіберзлочинності» [Електронний ресурс]: Офіційний сайт незалежної асоціації банків в Україні . – Режим доступу: http://anticyber.com.ua/news_detail.php?id=604

22. Риски в сети [Електронний ресурс]. – Режим доступу: http://xn--b1afankxqj2c.xn--p1ai/riski-v-seti

23. Садовська Є.В. Міжнародний досвід у боротьбі із загрозами інформаційній безпеці - уроки для України [Електронний ресурс] / Є.В. Садовська. – Режим доступу: http://goo.gl/Bpsn9u

24. Спам и фишинг [Електронний ресурс]: Офіційний блог компанії «Лабораторія Касперського». – Режим доступу: http://www.kaspersky.ru/internet-security-center/threats/spam-phishing

25. Худяков О. Как бороться с Интернет-мошенничеством? [Електронний ресурс] / О. Худяков. – Режим доступу: http://www.kp.ru/daily/26212/3096899/

26. Фишинг: кража персональных данных [Електронний ресурс]: Офіційний сайт антивірусної лабораторії Panda. – Режим доступу: http://www.viruslab.ru/security/types_malware/phishing

27. Что такое кибербуллинг? [Електронний ресурс]: Портал родителей Казахстана. – Режим доступу: http://www.ya-mama.kz/articles/Shkolniki/CHto_takoe_kiberbulling/view

28. Як захиститися від шахрайства в Мережі [Електронний ресурс]: Офіційний сайт незалежної асоціації банків в Україні . – Режим доступу: http://anticyber.com.ua/article_detail.php?id=239

29. A Quick Guide To Keeping Students Safe Online [Електронний ресурс]. – Режим доступу: http://www.edudemic.com/quick-guide-keeping-students-safe-online

30. Anti Mobbing [Електронний ресурс]: Громадська ініціатива у соціальній мережі Facebook. – Режим доступу: https://www.facebook.com/pages/Anti-Mobbing/222306871144717?ref=ts&fref=ts

31. Cyber-Mobbing – was ist das? [Електронний ресурс]. – Режим доступу: http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das

32. Net Losses: Estimating the Global Cost of Cybercrime [Електронний ресурс]. – Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

33. NetPolice: Правила компьютерной безопасности [Електронний ресурс]. – Режим доступу: http://www.netpolice.ru/safetips/spam

34. Online investigative principles for Federal law enforcement agents: Final Version (November 1999) [Електронний ресурс]. – Режим доступу: https://publicintelligence.net/department-of-justice-online-investigative-principles-for-federal-law-enforcement-agents

35. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. – Bedfordshire: ACPO NPIA, 2009. – 57 p.

36. What is cyberbullying, exactly? [Електронний ресурс]. – Режим доступу: http://stopcyberbullying.org/what_is_cyberbullying_exactly.html

37. 11 Facts About Cyber Bullying [Електронний ресурс]. – Режим доступу: https://www.dosomething.org/facts/11-facts-about-cyber-bullying

ДОДАТОК А

Основні правила Інтернет-безпеки для батьків

1. Перш, ніж дозволити дитині користуватися Інтернетом, розкажіть йому про можливі небезпеки Мережі (шкідливі програми, небезпечні сайти, Інтернет-шахраї тощо) і їх наслідки.
2. Чітко визначте час, який Ваша дитина може проводити в Інтернеті, і сайти, які він може відвідувати.
3. Переконайтеся, що на комп'ютерах встановлені і правильно налаштовані антивірусні програми, засоби фільтрації контенту і небажаних повідомлень.
4. Контролюйте діяльність дитини в Інтернеті за допомогою спеціального програмного забезпечення. Запитуйте дитину про те, що вона бачила у Інтернеті.
5. Поясніть дитині, що при спілкуванні в Інтернеті (чати, форуми, сервіси миттєвого обміну повідомленнями, онлайн-ігри) та інших ситуаціях, що вимагають реєстрації, не можна використовувати реальне ім’я. Допоможіть дитині вибрати реєстраційне ім’я, яке не містить ніякої особистої інформації.
6. Поясніть дитині, що не можна розголошувати в Інтернеті інформацію особистого характеру (номер телефону, домашню адресу, назву / номер школи тощо), а також «показувати» свої фотографії.
7. Допоможіть дитині зрозуміти, що далеко не все, що він може прочитати або побачити в Інтернеті - правда.
8. Поясніть дитині, що не можна відкривати файли, отримані від невідомих користувачів, так як вони можуть містити віруси або фото / відео з негативним змістом.
9. Привчіть дитину радитися з дорослими і негайно повідомляти про появу небажаної інформації.
10. Не дозволяйте Вашій дитині зустрічатися з онлайн-знайомими без Вашого дозволу або у відсутності дорослої людини.
11. Постаратися регулярно перевіряти список контактів своїх дітей. Поясніть дітям, що при спілкуванні в Інтернеті, вони повинні бути дружелюбними з іншими користувачами, ні в якому разі не писати грубих слів - читати грубості також неприємно, як і чути.

12. Поясніть дитині, шо потрібно періодично міняти паролі (наприклад, від електронної пошти, від профілів у соціальних мережах), але не слід використовувати занадто прості паролі, які можна легко зламати (дати народження, номери телефонів і т.ін.).

13. Розкажіть дитині, що якщо вона користується Інтернетом за допомогою чужого пристрою, то потрібно не забувати виходити зі свого облікового запису в соціальній мережі, в пошті і на інших сайтах після завершення роботи. Ніколи не слід зберігати на чужому комп'ютері свої паролі, особисті файли, історію листування.

Що робити, якщо дитина вже зіткнулася з будь-якою Інтернет-загрозою?

1. Встановіть позитивний емоційний контакт з дитиною, постарайтеся налаштувати її на розмову про те, що сталося. Дитина повинна вам довіряти і розуміти, що ви хочете розібратися в ситуації і допомогти їй, але ні в якому разі не покарати.

2. Якщо дитина засмучена чимось побаченим (наприклад, хтось зламав його профіль у соціальній мережі) або вона потрапила у неприємну ситуацію (витратила гроші в результаті Інтернет-шахрайства та ін.), постарайтеся заспокоїти її і разом розберіться в ситуації. З'ясуйте, що призвело до даного результату – безпосередньо дії самої дитини, недостатність Вашого контролю або незнання дитиною правил безпечної поведінки в Інтернеті.

3. Якщо ситуація пов'язана з насильством в Інтернеті щодо дитини, то необхідно дізнатися інформацію про кривдника, історію їх взаємин, з'ясувати, чи існує домовленість про зустріч в реальному житті і чи траплялися подібні зустрічі раніше, дізнатися про те, що відомо кривднику про дитину (реальне ім'я, прізвище, адресу, телефон, номер школи і т. п.).

4. Зберіть найбільш повну інформацію про подію – як зі слів дитини, так і за допомогою технічних засобів. Зайдіть на сторінки сайту, де була дитина, подивіться список друзів, прочитайте повідомлення. При необхідності скопіюйте і збережіть цю інформацію – в подальшому це може вам стати в нагоді для звернення до правоохоронних органів.

ДОДАТОК Б

БЕЗПЕКА ONLINE ПОКУПОК (ІНФОГРАФІКА)[15]

Крок № 1

[15] Джерело: http://lifehacker.ru/2013/03/12/infographics-online-shopping-security

Крок № 2


ВЫБЕРИТЕ МАГАЗИН
магазин
Если опыта покупок в новом интернет-магазине пока нет, постарайтесь узнать о нем побольше. Посоветуйтесь с друзьями или поищите отзывы в сети. Отсутствие отзывов — очень плохой признак!
Обратите внимание на сайт в целом. Если что-то вызывает сомнения, просто найдите альтернативу. Нужный товар есть еще в сотне других интернет-магазинов.
Старайтесь делать покупки в надежных и проверенных интернет-магазинах или официальных магазинах брендов.
Обратите внимание на внешний вид сайта – китайские сайты иногда копируют дизайн сайтов западных онлайн магазинов. Если замечаете, что это — сайт-копия, то лучше воздержаться от покупки.

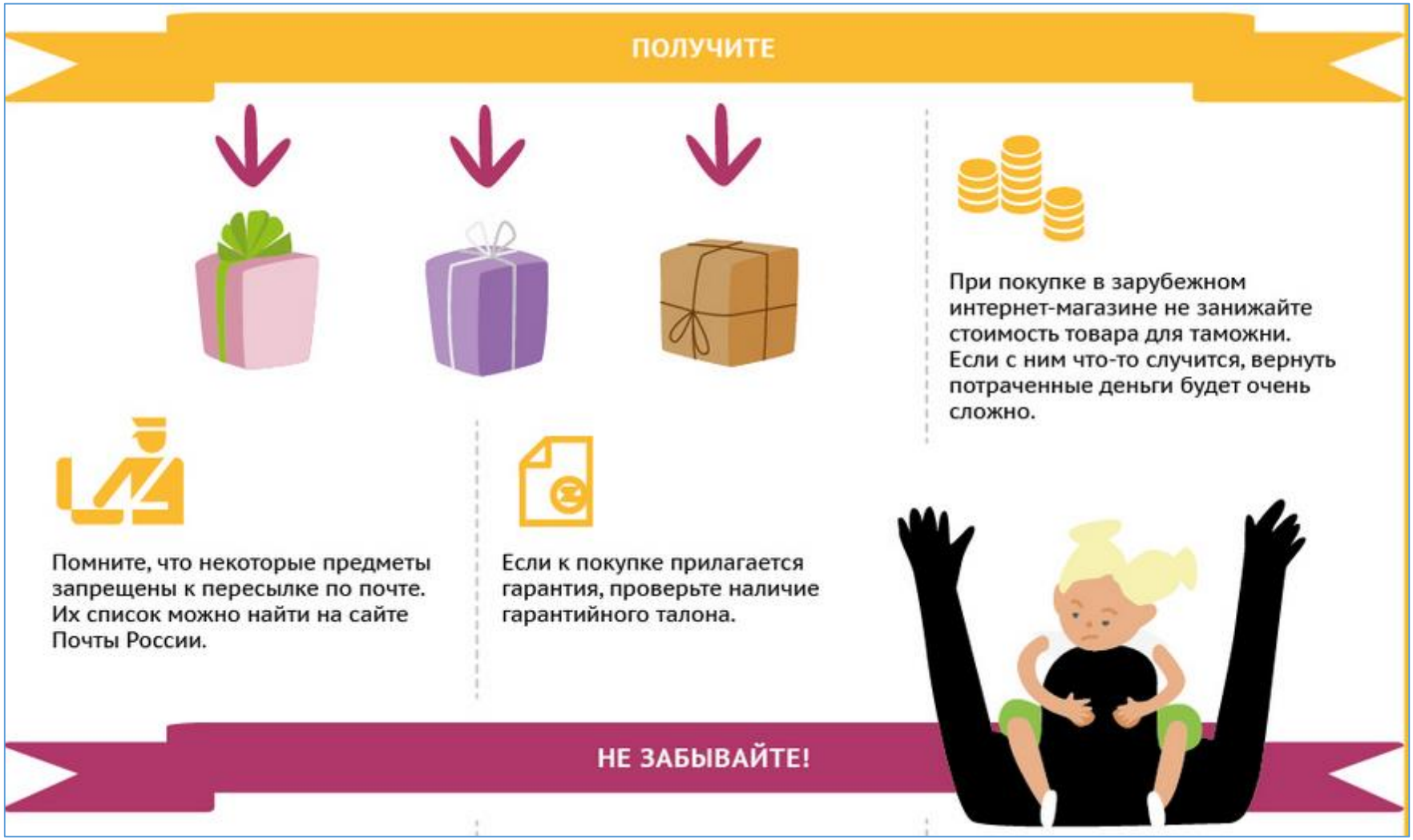
Крок № 3


СДЕЛАЙТЕ ПОКУПКУ
Перед покупкой узнайте общий уровень цен. Не обольщайтесь на слишком дешевые предложения незнакомых сайтов.
Помните, только на цену ориентироваться не стоит. Как правило, к ней придется добавить стоимость доставки.
Не забудьте проверить условия доставки, и главное — условия возврата.
Имейте ввиду, что товар может выглядеть не так, как вы ожидаете. Постарайтесь увидеть его заранее в обычном магазине.

Крок № 4


ОПЛАТИТЕ
Оплачивайте покупки только на тех сайтах, которым по-настоящему доверяете. Не забывайте собирать их в закладки.
https
Убедитесь в том, что все ваши транзакции происходят на защищенных страницах, обычно это обозначается замочком в строке браузера.
Verified by VISA
MasterCard. SecureCode.
При проведении оплаты обращайте внимание на наличие защиты от платежных систем Verified by Visa и MasterCard SecureCode. Их значки должны быть на сайте.
Будьте внимательны к названию сайта, на котором происходит оплата. Если вы идете на сайт Альфа-Банка, и вместо alfabank.ru отображается alphabanc.ru или что-то подобное — насторожитесь, скорее всего, это ловушка кибер-преступников.
Если перед оплатой у вас все еще остались какие-либо сомнения, по возможности оплатите первую покупку наличными курьеру при получении. Это убережет от мошенничества и подделок.

Крок № 5


ПОЛУЧИТЕ
При покупке в зарубежном интернет-магазине не занижайте стоимость товара для таможни. Если с ним что-то случится, вернуть потраченные деньги будет очень сложно.
Помните, что некоторые предметы запрещены к пересылке по почте. Их список можно найти на сайте Почты России.
Если к покупке прилагается гарантия, проверьте наличие гарантийного талона.
НЕ ЗАБЫВАЙТЕ!

Додаток В

Приклади адміністративних правопорушень, пов’язаних із ризиками мережі Інтернет.
На увазі мається те, що діяльність осіб, що здійснюють протиправні дії в Інтернет, може бути розцінена, як адміністративне правопорушення відповідної категорії

Контентні ризики – це матеріали (тексти, зображення, аудіо, відеофайли, посилання на сторонні ресурси), що містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.ін.	**Стаття 51-^{2}. Порушення прав на об'єкт права інтелектуальної власності** Незаконне використання об'єкта права інтелектуальної власності (літературного чи художнього твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом. **Стаття 156-^{3}. Порушення встановлених законодавством вимог щодо заборони реклами та спонсорства тютюнових виробів** Реклама, а так само будь-яка інша діяльність з рекламування тютюнових виробів, знаків для товарів і послуг, інших об’єктів права інтелектуальної власності, під якими випускаються тютюнові вироби, з порушенням вимог чинного законодавства про рекламу. **Стаття 164-^{6}. Демонстрування і розповсюдження фільмів без державного посвідчення на право розповсюдження і демонстрування фільмів** Демонстрування фільмів або розповсюдження фільмів шляхом продажу чи передачі в прокат фільмокопій без державного посвідчення на право розповсюдження і демонстрування фільмів.
Електронні (кібер-) ризики – це можливість зіткнутися з розкраданням персональної інформації, ризик піддатися вірусній атаці, онлайн-шахрайству, спам-атаці, шпигунським програмам і т.ін.	**Стаття 212-^{6}. Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем** Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах.

Споживчі ризики – зловживання в Інтернеті правами споживача. Вони включають в себе: ризик придбання товару низької якості, контрафактної і фальсифікованої продукції, втрата коштів без придбання товару або послуги, викрадення персональної інформації з метою кібершахрайства, та ін.	**Стаття 155-^{2}. Обман покупця чи замовника** Обмірювання, обважування, обраховування, перевищення встановлених цін і тарифів або інший обман покупця чи замовника працівниками торгівлі, громадського харчування і сфери послуг та громадянами - суб'єктами підприємницької діяльності під час реалізації товарів, виконання робіт, надання послуг. **Стаття 156-^{1}. Порушення законодавства про захист прав споживачів** Відмова працівників торгівлі, громадського харчування та сфери послуг і громадян, які займаються підприємницькою діяльністю в цих галузях, у наданні громадянам-споживачам необхідної, доступної, достовірної та своєчасної інформації про товари (роботи, послуги), їх кількість, якість, асортимент, а також про їх виробника (виконавця, продавця), у навчанні безпечного та правильного їх використання, а так само обмеження прав громадян-споживачів на перевірку якості, комплектності, ваги та ціни придбаних товарів – **Стаття 164. Порушення порядку провадження господарської діяльності** Провадження господарської діяльності без державної реєстрації як суб'єкта господарювання або без одержання ліцензії на провадження певного виду господарської діяльності, що підлягає ліцензуванню відповідно до закону, чи здійснення таких видів господарської діяльності з порушенням умов ліцензування, а так само без одержання дозволу, іншого документа дозвільного характеру, якщо його одержання передбачене законом (крім випадків застосування принципу мовчазної згоди)

Приклади злочинів, пов’язаних із ризиками мережі Інтернет.
На увазі мається те, що діяльність осіб, що здійснюють протиправні дії в Інтернет, може бути розцінена, як злочин відповідної категорії

Контентні ризики – це матеріали (тексти, зображення, аудіо, відеофайли, посилання на сторонні ресурси), що містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.ін.	**Стаття 176. Порушення авторського права і суміжних прав** Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у значному розмірі. **Стаття 300. Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію** Ввезення в Україну творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою або їх збут чи розповсюдження, а також примушування до участі в їх створенні. **Стаття 301. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів** Ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні. **Стаття 307. Незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів** Незаконне виробництво, виготовлення, придбання, зберігання, перевезення чи пересилання з метою збуту, а також незаконний збут наркотичних засобів, психотропних речовин або їх аналогів.

	Стаття 258-2. Публічні заклики до вчинення терористичного акту Публічні заклики до вчинення терористичного акту, а також розповсюдження, виготовлення чи зберігання з метою розповсюдження матеріалів з такими закликами. **Стаття 436. Пропаганда війни.** Публічні заклики до агресивної війни або до розв'язування воєнного конфлікту, а також виготовлення матеріалів із закликами до вчинення таких дій.
Комунікаційні ризики пов'язані з міжособистісними відносинами Інтернет-користувачів і включають в себе ризик піддатися образам і нападкам з боку інших. Прикладами таких ризиків можуть бути: незаконні контакти (наприклад, грумінг), кіберпереслідування, кібербулінг та ін	**Стаття 120. Доведення до самогубства** Доведення особи до самогубства або до замаху на самогубство, що є наслідком жорстокого з нею поводження, шантажу, примусу до протиправних дій або систематичного приниження її людської гідності. **Стаття 154. Примушування до вступу в статевий зв'язок** Примушування жінки чи чоловіка до вступу в статевий зв'язок природним або неприродним способом особою, від якої жінка чи чоловік матеріально або службово залежні. **Стаття 155. Статеві зносини з особою, яка не досягла статевої зрілості** Статеві зносини з особою, яка не досягла статевої зрілості. **Стаття 156. Розбещення неповнолітніх** Вчинення розпусних дій щодо особи, яка не досягла шістнадцятирічного віку, -
Електронні (кібер-) ризики – це можливість зіткнутися з розкраданням персональної інформації, ризик піддатися вірусній атаці, онлайн-шахрайству, спам-атаці, шпигунським програмам і т.ін.	**Стаття 190. Шахрайство** Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки. **Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення** Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей.

	Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності. **Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку** Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. **Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. **Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації** Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. **Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку**

	Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.
Споживчі ризики – зловживання в Інтернеті правами споживача. Вони включають в себе: ризик придбання товару низької якості, контрафактної і фальсифікованої продукції, втрата коштів без придбання товару або послуги, викрадення персональної інформації з метою кібершахрайства, та ін.	**Стаття 190. Шахрайство** Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки. **Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю** Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності.