УДК 342.9:5.08(477)

Яна Ігорівна Фещенко,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. юрид. наук Коломоєць Н. В.

УМОВИ БЕЗПЕЧНОГО КОРИСТУВАННЯ ІНТЕРНЕТОМ

За декілька останніх десятиліть людство істотно змінило спосіб життя завдяки розвитку новітніх технологій. Сучасність демонструє, що з появою всесвітньої мережі Інтернет технічні пристрої стали невід'ємною частиною людського життя. Так, наприклад, письмові скриньки замінено електронною поштою, стаціонарні телефони – мобільними, стаціонарні комп'ютери – ноутбуками. Також, у нашому користуванні з'явилося все більше нових і доступних пристроїв: планшети, портативні комп'ютери, нетбуки тощо. За допомогою цих пристроїв люди майже постійно підключаються до Інтернету, реалізуючи свої потреби та цілі. Всі новітні пристрої мають свої властивості та функції, але найпоширенішою серед них є така, що надає можливість користувачу спілкуватися з іншими людьми через Всесвітню мережу. Разом з тим, найбільшої популярності у користувачів набули соціальні мережі. Завдяки соціальним мережам доступним і оперативним стало не лише спілкування, а й перегляд фотографій, відеозаписів, новин тощо.

Тим часом, можливість оперативного доступу до інформації отримали хакери та інтернет-шахраї. Наразі, однією з найпоширеніших загроз є фішинг. Фішингом є один із видів шахрайства, який полягає в отриманні персональних даних користувача завдяки його довірливості або неуважності. Фішингові атаки, наразі, є поширеною формою зараження комп'ютерів шкідливими програмами, тобто програмами, які приховують свою присутність на комп'ютері і можуть бути використані для управління зараженим комп'ютером, крадіжки інформації або стеження за користувачем. Зловмисник, як правило, надсилає таке фішингове повідомлення, яке мотивує користувача перейти за посиланнями та відкрити додані файли, які можуть містити загрозу. Для фішингу частіше використовується інтернет-чат. Тому важливо перевіряти посилання, одержувані на електронну пошту або в чаті.

Веб-адреси в електронних листах можуть бути оманливими. Надіслана в листі веб-адреса може містити посилання на зовсім інший веб-сайт. Таким чином відбувається зараження комп'ютера та отримання інтернет-шахраями персональних даних користувача, нібито, не порушуючи правила конфіденційності.

Беручи до уваги, що персональні дані користувачів являють собою не лише інформацію, необхідну для доступу до особистої сторінки користувача у соціальній мережі, а й для здійснення інтернет-банкінгу, необхідно бути уважним і пам'ятати головні правила безпечного користування інтернет-ресурсами.

Разом з тим, ще неможливо повністю застерегти себе від дії інтернет-шахраїв, але наступні 10 порад допоможуть прийняти ефективні заходи для того, аби не стати їх жертвою:

1. Необхідно бути уважними при використанні інтернет-посилань, які користувач отримує від своїх друзів у соціальних мережах. З даними посиланнями необхідно поводитися так, як і з незнайомими та такими, які отримує користувач на адресу електронної пошти.

2. Необхідно запам'ятовувати особисті данні, які вводить користувач. Як правило, хакери отримують незаконний доступ до фінансових або інших рахунків використовуючи посилання «Забули свій пароль?» на реєстраційній інтернет-сторінці рахунку. Задля того, щоб отримати доступ до рахунку, хакери підбирають відповіді на секретні питання. Такими класичними питаннями є: рік народження користувача; назва рідного міста або вулиці; ім'я кращого друга дитинства; прізвисько домашньої тварини; дівоче прізвище матері тощо. Рекомендовано створювати власні контрольні питання, якщо таке можливо відповідно до параметрів сайту. Але слід пам'ятати, що дана інформація не має бути у відкритому доступі.

3. Не слід вірити тому, що повідомлення дійсно надійшло від того відправника, ім'я якого вказано у повідомленні. Хакери можуть отримати доступ до рахунків інших осіб та відправляти повідомлення від їхнього імені. Якщо у користувача виник сумнів стосовно дійсності даного повідомлення, рекомендовано зв'язатися з відправником через інші альтернативні засоби зв'язку (наприклад, зателефонувати) та запитати чи надсилав він дане повідомлення. Такі повідомлення можуть виглядати як запрошення від друга приєднатися до нової соціальної мережі.

4. Для запобігання розголошенню адреси електронної пошти друзів, не треба дозволяти службам соціальних мереж сканувати контактні дані. Наприклад, коли користувач приєднується до нової соціальної мережі, йому можуть запропонувати ввести адресу своєї електронної пошти або пароль, задля того, щоб дізнатися чи зареєстрований даний контакт в мережі. Сайти можуть використовувати цю інформацію для розсилки повідомлень по всім контактам користувача, використовуючи при цьому електронну адресу останнього.

5. Адресу соціальної мережі необхідно вводити власноруч або використовуючи особисті закладки. При вході на веб-сторінку через повідомлення, яке надійшло на електронну пошту, користувач може ввести особисті дані на фішинговий сайт, звідки вони можуть бути викрадені інтернет-шахраями.

6. Необхідно бути особливо уважним при долученні друзів у соціальних мережах. Інтернет-шахраї можуть створювати фейкові сторінки для отримання від користувача необхідної для них інформації.

7. Також, необхідно бути обережним при виборі соціальної мережі. Спочатку треба ознайомитися з правилами користування даним сайтом, які пропонує адміністратор та впевнитися у тому, що особиста інформація користувача матиме конфіденційний характер та не буде використана в інших цілях.

8. Особисті дані користувача залишаються на сайті соціальної мережі назавжди. Навіть після видалення особистого профілю, дані, які користувач завантажував, зберігаються на інтернет-сервері і можуть бути використані для інших цілей хакерами.

9. Більшість сайтів соціальних мереж автоматично завантажують програми інших розробників, що в подальшому слугує можливістю для хакерів викрасти особисті дані користувача, використовуючи такі програми. Для безпечного скачування і використання таких програм необхідно використовувати традиційні запобіжні заходи.

10. Важливо, також, вимкнути функцію геолокації фотознімків.

Одержано 20.04.2017

УДК 347.963

Валентина Володимирівна Подріз,
курсант 3 курсу факультету № 1 ХНУВС
Науковий керівник: канд. юрид. наук Невядовський В. О.

ЩОДО ВИЗНАЧЕННЯ ПОНЯТТЯ СУБ'ЄКТІВ КООРДИНАЦІЇ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Першочерговим завданням системи правоохоронних органів України є втілення у життя, захист та забезпечення ключових положень Конституції України, особливо в частині прав та свобод людини і громадянина. У вищенаведеній сфері залишається ще багато дискусійних питань. Зокрема, не достатньо уваги приділено поняттю та сутності суб'єктів координації правоохоронної діяльності.

Аналіз правової літератури дозволив зробити висновок про відсутність достатньої кількості визначень терміну «суб'єкт координації». Є лише поодинокі спроби ряду науковців наповнити певним змістом дане поняття, прямо чи опосередковано ведучи мову про перелік органів, які можна віднести до суб'єктів координації. Більш того, такий перелік є різним в залежності від сфери координації. Отже, у своєму дослідженні Д. К. Єфіменко аналізуючи ключові поняття «суб'єкт» та «координація» дійшов висновку про те, що під суб'єктами координації слід розуміти суб'єктів права, які уповноважені державою на здійснення координації [1, с. 173]. Розширюючи даний термін науковець асоціює його із органами державної влади та посадовими особами, до компетенції яких законодавством віднесено права й обов'язки щодо розробки і реалізації заходів по узгодженню діяльності різних ланок правоохоронного механізму [1, с. 175]. Аналогічну ситуацію з приводу терміну «суб'єкт координації», а саме відсутність чіткого та зрозумілого терміну, спостерігаємо і в нормативно-правовому полі. Так, серед нормативно-правових актів законодавчого рівня даного визначення віднайти не представилося можливим. Такий результат є прогнозованим через деталізацію терміну, що не характерна для рівня закону України. А от на рівні підзаконних нормативно-правових актів є певні напрацювання. Зокрема, Порядок складання та подання запитів на отримання публічної інформації, що знаходиться у володінні органів Державної