УДК 004.056.55

Луканов М.В.
Шелепало Г.В.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТ-МЕРЕЖІ. КІБЕРГІГІЄНА У СОЦІАЛЬНИХ МЕРЕЖАХ.

Вінницький національний технічний університет

Анотація

В даній статі розглянуто питання захисту персональних даних в мережі інтернет. Проаналізовано сучасний стан загального рівня безпеки у соціальних мережах, інтернет магазинах, форумах та інших сервісів, якими користуються люди різних вікових категорій. Прохарактеризовано основні загрози, які виникають під час користування інтернетом. Запропоновано модель поведінки користувача у соціальних мережах, враховуючи правила кібергігієни з їх обґрунтуванням та представленням актуальності.

Ключові слова: Інтернет, користувач, особисті дані, загрози, кібергігієна, соціальні мережі, запобігання загроз.

Abstract

This article discusses the protection of personal data on the Internet. The main threats to the user and methods of their prevention are characterized. A model of user behavior in social networks is proposed, taking into account the rules of cyber hygiene.

Key words: Internet, user, personal data, threats, cyber hygiene, social networks, threat prevention, pattern of behavior.

Вступ

Кожного дня цифрові технології поглинають ще більше сфер нашого життя, стають невід'ємною частиною буднів сучасної людини. На сьогодні майже кожен має власний смартфон з доступом до інтернет-мережі, це дозволяє користувачам бути онлайн практично завжди. Так, ви можете в будь-яку секунду переглянути баланс банківської картки, купити квиток на потяг чи в кінотеатр, перевірити пошту та соціальні мережі на наявність нових повідомлень, здійснювати покупки та інші фінансові операції користуючись лише смартфоном. Всі ці дії в інтернеті передбачають обмін тою чи іншою особистою інформацією чи конфіденційними даними, які через необережність можуть потрапити до рук зловмисників.

Основна частина

В 32 статті Конституції України закріплено положення про те, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України, не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1]. Отже, втручання в особисте життя та заволодіння конфіденційною інформацією є протиправним дійством та карається законом. На жаль, це зупиняє далеко не всіх, тому кожному необхідно знати, як захищати особисту інформацію.

Для максимально надійної протидії злочинцям необхідно дотримуватися певних правил поводження в інтернеті, слідкувати за особистою гігієною у віртуальному світі, розуміти, що твоя особиста безпека в твоїх руках. Щоб не потрапити під вплив злочинців, необхідно знати про такі основні загрози:

• Загроза порушення конфіденційності. Вона полягає в тому, що дані стають відомими тим, хто не має права доступу до них та виникає щоразу, коли отримано доступ до деяких секретних даних, що зберігаються в комп'ютерній системі чи передаються від однієї системи до іншої.

• Загроза порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу. Вона виникає, коли зловмисники навмисно змінюють дані, тобто порушується їхня цілісність.

• Загроза відмови служб (загроза доступності) виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп'ютерної системи. Блокування буває постійним, якщо доступ до запитуваного ресурсу ніколи не буде отримано, або воно може викликати тільки затримку запитуваного ресурсу, досить довгу для того, щоб він став непотрібним. У цих випадках говорять, що ресурс вичерпано [2].

Так як в наш час молодь, як правило, більшість часу в інтернеті проводить у соціальних мережах вирішено створити збірку правил та рекомендацій для запобігання вищевказаних загроз.

Як правило, сучасна молодь більшість часу в інтернеті проводить у соціальних мережах, тому було вирішено створити збірку правил та рекомендацій для запобігання вищевказаних загроз

Правило перше - нікому не повідомляйте особисті дані. Ніколи. Зловмисники можуть вдаватися до різноманітних схем, наприклад, повідомляти, що саме ви отримали великий приз, але для його отримання необхідний ваш номер телефону, банківська картка, тощо. Є випадки, коли злочинець отримує доступ до сторінки вашого знайомого та пише від його імені, просить позичити гроші, надати певну конфіденційну інформацію та інше.

Правило друге - перевіряйте інформацію. Не поширюйте новини із занадто гучними заголовками. Можливо, це фейк. Перевірте: спитайте в знайомих, які розбираються в цій темі, або перегляньте новинну стрічку інших сайтів. Також не менш важливо перевіряти інформацію, якщо вас просять пожертвувати гроші на якусь операцію чи зробити репост посту із новиною подібного змісту. Пам'ятайте, шахраї часто видають себе за благодійників. Ця звичка буде корисна не лише в інтернеті, а й у реальному житті.

Правило третє - захищайте паролі. До цього правила відноситься відразу декілька порад. В першу чергу, ніколи не використовуйте однакові паролі для різних сайтів, є можливість, що зловмисник скористається вразливістю одного сайту та дізнається пароль до ваших облікових записів різних сервісів. По-друге, користуйтеся складними паролями, їх важче підібрати, для цього використовуйте букви різних регістрів, цифри та дозволені знаки одночасно, а його довжина має бути не менше ніж 12 символів. Третя порада – регулярно міняйте паролі, чим частіше, тим краще, але не забувайте про дві попередні поради. І на останнє – якщо вам важко запам'ятати велику кількість паролів, не записуйте їх в блокнот чи зошит, краще користуйтеся спеціальними менеджерами паролів, але при скачуванні звертайте увагу на їх рейтинг та відгуки [3].

Правило четверте - використовуйте двофакторну автентифікацію усюди, де це можливо. Ця операція не займе багато часу, окрім паролю, вам зателефонують або надішлють код, так ваші дані в мережі будуть ще більш убезпечені. Також рекомендуємо завершувати сеанс одразу після виходу із соціальної мережі.

Правило п'яте - видаліть свої критично важливі дані з соціальних мереж. Багато банків при голосовому дзвінку запитують у клієнтів додаткову інформацію. Краще переконатися, що ви не розмістили слово-пароль у відкритому доступі. Тому краще не вказувати дату народження, кличку домашнього вихованця або дівоче прізвище матері - все те, що використовується при доступі до фінансових сервісів.

Правило шосте – використовуйте інтернет-картки при покупках онлайн. Для цього створіть картку у додатку банку та при онлайн шопінгу переводьте на цю картку необхідну суму та вже з неї оплачуйте покупки, це збереже ваші кошти у випадку, коли зловмисник дізнається дані картки, яку ви використали в онлайн магазині.

Правило сьоме – закривайте старі облікові записи. Якщо ви знаєте, що більше не будете користуватися певним сайтом, видаліть на ньому свій акаунт, це зменшить ваш цифровий слід та ускладнить роботу можливим зловмисникам.

Правило восьме – перевіряйте сайти. Перш ніж купувати якусь річ, переводити кошти чи завантажувати файли, знайдіть якомога більше відгуків про цей сайт, можливо знайдете інформацію про його шахрайську діяльність, в такому випадку більше не користуйтеся ним [4].

Правило дев'яте - регулярне оновлення. Як тільки виходить нова версія ваших додатків, операційної системи смартфонів чи персонального комп'ютера, оновлюйте його, але не забудьте перевірити новину про оновлення на правдивість та при завантаженні використовуйте лише офіційні сайти від виробника продукції.

Правило десяте – використовуйте VPN. Якщо ви використовуєте Wi-Fi в публічному місці, ваш трафік може перехопити зловмисник. У таких місцях краще захистити себе за допомогою сервісу VPN.

В цих десятьох правилах зібрано саме основні вимоги до особистої безпеки в інтернет мережі, якщо ідеально дотримуватися їх ризик стати жертвою кіберзлочину значно зменшується, але не дорівнює нулю. Саме тому можна запропонувати ще одне, додаткове правило – не стійте на місці. Злочинець завжди вдосконалюється, для успішного злочину йому необхідно бути на рівень вище системи та об'єкту захисту, що й вимагає від нього постійного вдосконалення. Отже, для того, щоб ефективно захищати себе від інтернет шахраїв, вірусів та інших небезпек необхідно також не забувати про самовдосконалення, покращення своїх знань та навичок.

Висновки

Отже, враховуючи сучасні тенденції, навички безпечної поведінки в інтернеті вкрай важливі як для активного користувача мережі, так і для тих, хто користується нею не часто, адже кожен може стати жертвою зловмисників і понести фінансові чи моральні втрати. Користуючись поданими правилами у повсякденному житті ви зможете захистити себе та вберегти від небезпеки інших, головне не забувати, що ваша безпека залежить від вас.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конституція України [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Загрози при роботі в Інтернеті і їх уникнення [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/informacijnesuspilstvo26/informacijni-tehnologiie-u-suspilstvi/urok-4-zagrozi-pri-roboti-v-interneti-i-ieh-uniknenna Конституція України [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
3. 1. ДаникЮ. Г., ГрищукР. В. Основи кібернетичної безпеки : монографія. Житомир : ЖНАЕУ, 2016. 636 с.
4. Даник Ю. КІБЕРОСВІТА ТА ЇЇ ОСОБЛИВОСТІ : дис. докт. техн. наук / Даник Юрій, 2019. – 17 с.

Луканов Максим Всеволодович – студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail max.luk.2001@gmail.com

Науковий керівник: ***Шелепало Галина Василівна*** – кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail nv.shelepalo@vntu.edu.

Lukanov Maksym Vsevolodovich - student of kits-19B group, Faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail max.luk.2001@gmail.com

Supervisor: ***Shelepalo Halyna Vasylivna*** - Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail hv.shelepalo@vntu.edu.ua