УДК 004.58:004.77

Д. В. СОКОЛ, студентка, А. В. КОЗИКОВ, ст. викладач
Криворізький національний університет

ПРОБЛЕМИ, ПОВ'ЯЗАНІ З БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ, ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Через швидкий технологічний розвиток та стрімке поширення мобільних пристроїв, їхнє використання стало невід'ємною частиною нашого повсякденного життя. Ми користуємось ними для роботи, покупок, розваг і спілкування з рідними та друзями. Проте з кожним роком зростає кількість злочинних посягань на безпеку мобільних пристроїв, які можуть призвести до витоку конфіденційної інформації у мережу Інтернет, крадіжки особистих даних з метою шантажу чи викрадення грошей з банківських рахунків. Нині повномасштабне вторгнення на територію нашої країни супроводжується підвищеною агресією у кіберпросторі [1], атакам піддаються не лише державні установи, а й мобільні пристрої політиків, військових і простих мирних жителів. Тож зараз питання кібергігієни є актуальним як ніколи. Проблеми безпеки мобільних пристроїв можуть виникнути і з багатьох інших причин, включаючи недобросовісність компаній-виробників та недостатні заходи безпеки з боку користувачів. Однак, на щастя, існують певні стратегії та практики, які можна використовувати для захисту гаджетів від потенційних небезпек.

Розглянемо детальніше загрози, які підстерігають користувачів мобільних пристроїв, та дізнаємося причини їхнього виникнення. Втрата особистих даних може статися через недбале ставлення до оновлень ПЗ – багато людей думають, що цей етап неважливий, бо змінюється лише UI-дизайн, але, насправді, розробники виправляють помилки та оновлюють системи безпеки, щоб убезпечити особисті дані своїх клієнтів. Завантажуючи застосунки та файли з ненадійних джерел, користувачі можуть отримати віруси або шкідливі програми, які можуть викрасти або пошкодити персональні дані. Крадіжка або випадкова втрата мобільного пристрою може призвести до недоступності особистої інформації або навіть її компрометації. Підключення до відкритих або незахищених Wi-Fi мереж теж може стати причиною перехоплення особистої інформації зловмисниками. Ще одна небезпека для користувачів – соціальний інжиніринг – у шахраїв більше шансів отримати конфіденційну інформацію, використовуючи псевдоніми співробітників компаній або відомості зі службових ресурсів, щоб виглядати більш впевнено. Джейлбрейкінг («jailbreaking») для iOS і рутінг («rooting») для Android знімають обмеження виробників, розширюють можливості користувачів, але роблять пристрої беззахисними перед різними загрозами.

Як же захистити свої гаджети? Слід завантажувати застосунки та файли лише з офіційних магазинів або з сайтів відомих розробників. Щоб убезпечити пристрій від несанкціонованого доступу, рекомендується встановити надійний пароль та увімкнути шифрування даних, важливо, щоб паролі на всіх пристроях були різними. Необхідно використовувати VPN-з'єднання, при підключенні до незахищених Wi-Fi мереж, обираючи VPN-сервіси слід надавати перевагу тільки платним ліцензованим програмам, адже безкоштовні заробляють саме на продажі особистих даних користувачів. Щоб контролювати, яка інформація доступна іншим користувачам, потрібно перевірити налаштування конфіденційності соцмереж та електронної пошти, а отримавши листа з невідомими файлами чи посиланнями, у жодному разі не відкривати їх. Варто уникати джейлбрейкінгу та рутінгу, якщо ж без цього ніяк – працювати лише з офіційними програмами. Слід встановити антивірусну програму, якщо її не було одразу. Завжди варто бути уважними та обережними при спілкуванні.

Отже, аби зменшити ризики для безпеки при використанні мобільних пристроїв, користувачам слід дотримуватися кількох простих порад, які зазначені вище. Усе це, на жаль, не може гарантувати постійний 100% захист, адже рівень кіберзлочинності невпинно зростає, проте виконання практичних рекомендацій допоможе значно знизити загрозу втрати особистих даних. Безпека мобільних пристроїв – важлива тема, яку обов'язково треба висвітлювати на уроках та виховних годинах у школах, оскільки діти часто використовують гаджети для навчання, спілкування та розваг і можуть стати легкою здобиччю для зловмисників.

Список літератури

1. **Мальцева І. Р., Черниш Ю. О., Штонда Р. М.** Аналіз деяких кіберзагроз в умовах війни / **І. Р. Мальцева, Ю. О. Черниш, Р. М. Штонда** // Кібербезпека: освіта, наука, техніка, 2022, том 4 №16 – 193 с.