ними матеріалами виробничого процесу і оптимізувати час поставки матеріалів, значно знижуючи складські витрати.

ЯК ЗАХИСТИТИ ОСОБИСТІ ДАНІ В ІНТЕРНЕТІ

Чухов О.І.
Науковий керівник – ***Сенчук Т.С., асистент***

Дана робота покликана допомогти зрозуміти, чому наші персональні дані кожен день знаходяться під загрозою, і дати поради про те, як захистити особисту інформацію в мережі.

Зловмисники кожен день крадуть персональні дані знаменитостей і звичайних користувачів. Багато хто думає, що їх дані злочинцям не цікаві, але досвід показує, що популярність не впливає на бажання зловмисників отримати чужі персональні дані і витягти з них вигоду. В роботі приведені найпопулярніші сценарії, в яких ваші дані знаходяться під загрозою, і розглянемо, що робити, щоб зберегти особисту інформацію в таємниці.

Електронна пошта більше ніж просто поштова скринька. Ви використовуєте її для реєстрації на більшості сайтів і сервісів, а значить, отримавши доступ до пошти, зловмисники зможуть зламати і інші ваші акаунти. Ніхто не відміняв і загрозу таємниці листування. Якщо це робочий ящик, то до хакерів може потрапити закрита корпоративна інформація.

Акаунти в ігрових сервісах. Користувачі заробляють ігровий досвід, внутрішньо-ігрову валюту, купують за реальні гроші речі для ігрового інвентарю, самі ігри. Зламавши ваш ігровий акаунт, зловмисники вкрадуть куплені ліцензійні ігри, ігровий інвентар та предмети – і отримають за них реальні гроші.

Соціальні мережі та месенджери – кращі об'єкти для шахраїв, якщо вони хочуть поживитися інтимними подробицями вашого життя. Якщо ви грамотно не захистили свій акаунт, то біда може трапитися коли завгодно. Для багатьох листування в соціальних мережах і месенджерах замінює електронну пошту – вони обмінюються фотографіями, документами, інший конфіденційною інформацією.

Цифрова крадіжка смартфона. У всіх сучасних смартфонів є основній обліковий запис: для iOS це Apple ID, для Android – акаунт Google. Якщо зловмисники отримають до них доступ, цінна інформація про вас виявиться в їх руках.

Мобільні додатки (ігри) ці програми запитують доступ до даних: ваши контакти, геопозіція, календар, платіжні дані. Кожен раз уважно читайте, до якої інформації запитує доступ додаток або гра.

Зараз банківськими картами розплачуються не тільки в звичайному супермаркеті: картою оплачують комунальні послуги через інтернет-банк і покупки в онлайн-магазинах, за допомогою карти бронюють авіаквитки і готелі.

Wi-Fi - щастя для мандрівника і фрілансера. Але зловмисники користуються незахищеністю відкритих точок і необережністю користувачів. До речі, хакери підбираються і до запаролених точок. А там уже справа техніки: підключилися до Wi-Fi, і все, що ви робите на екрані і вводите на клавіатурі, бачить зловмисник.

Як бачите, проблема безпеки в інтернеті стає актуальнішою, ніж будь-коли. Скрізь є ризик попастися на вудку кібер-злочинців. Розповімо про основні способи захисту персональних даних, які обов'язково варто застосовувати на практиці.

Двухфакторна аутентифікація – це подвійний захист, перший рубіж якої, звичайна комбінація логіна і пароля, тобто те, що зберігається на сервері, а другий, те, до чого є доступ тільки у конкретного користувача. Для чого підійде: електронна пошта, акаунти в соціальних мережах і месенджерах, ігрові акаунти, акаунт для смартфона, інтернет-банк.

Захищене з'єднання. Здійснюючи покупки та інші потенційно небезпечні дії, зверніть увагу на значок ліворуч адресного рядка. Переконайтеся, що працюєте з сайтом по зашифрованому з'єднанню. Для чого підійде: електронна пошта, акаунти в соціальних мережах і месенджерах, ігрові акаунти, акаунт для смартфона, інтернет-банк.

Є спеціальні менеджери паролів, які беруть головний біль на себе. Вони самі генерують складні паролі, зберігають їх у захищеному сховище, а вам не потрібно пам'ятати про пароль до конкретного сайту - додаток саме підставить його в потрібне поле. Найпопулярніші сервіси: 1Password, LastPass, Enpass. Для чого підійде: електронна пошта, акаунти в соціальних мережах і месенджерах, ігрові акаунти, акаунт для смартфона, інтернет-банк.

Контролюйте доступ додатків до ваших даних. Користувачі iOS, а з недавніх пір і Android, можуть управляти доступом додатків до різних даних. Для чого підійде: мобільні додатки.

Користуйтеся VPN, працюючи з публічними Wi-Fi-точками

Працюючи в кафе та інших громадських місцях з Wi-Fi, користуйтеся VPN-сервісом. Він перенаправляє трафік на власний сервер, а вам віддасть вже «очищений», який не можуть відслідковувати зловмисники. Пам'ятайте, що доступ по паролю не гарантує безпеки.