Лабораторна робота − Дослідіть ризики своєї поведінки в Інтернеті

Цілі та задачі

Дослідити дії в Інтернеті, що можуть скомпрометувати вашу безпеку чи конфіденційність.

Довідкова інформація / Сценарій

Інтернет − це вороже середовище і ви повинні бути пильними, щоб ваші дані не були скомпрометовані. Зловмисники креативні і будуть використовувати різні методи, щоб обдурити користувачів. Ця лабораторна робота допоможе вам визначити ризики своєї поведінки в Інтернеті та надати поради щодо безпечного використання Інтернету.

Частина 1: Знайомимося з правилами надання послуг

Відповідайте на запитання, що наведені нижче, чесно та зверніть увагу, скільки балів дає кожна відповідь. Додайте всі отриманні бали щоб отримати результат та перейдіть до Частини 2 для аналізу вашої поведінки в Інтернеті.

a. Якою інформацією ви ділитеся на сайтах соціальних мереж? _____

1) Всією; Я покладаюся на соціальні мережі, щоб підтримувати зв'язок з друзями та родиною. (3 бали)
2) Статті та новини, які я знаходжу чи читаю (2 бали)
3) Це залежить від того чим і з ким я ділюся. Я відфільтровую. (1 бал)
4) Нічим. Я не використовую соціальні мережі. (0 балів)

b. Коли ви створюєте новий обліковий запис в онлайн-службі, ви: _____

1) Повторно використовуйте той самий пароль, який використовується в інших службах, щоб полегшити його запам'ятовування. (3 бали)
2) Створюєте пароль, який є максимально простим, щоб ви могли його запам'ятати. (3 бали)
3) Створюєте дуже складний пароль і зберігаєте його в службі керування паролями. (1 бал)
4) Створюєте новий пароль, який схожий, але відрізняється від пароля, який використовується в іншій службі. (1 бал)
5) Створюєте абсолютно новий надійний пароль. (0 балів)

c. Коли ви отримуєте електронне повідомлення з посиланнями на інші сайти: _____

1) Ви не натискаєте на посилання, тому що ви ніколи не переходите за посиланнями, що приходять вам у електронних повідомленнях. (0 балів)
2) Ви переходите за посиланням, тому що поштовий сервер вже просканував це повідомлення. (3 бали)
3) Ви переходите за всіма посиланнями, якщо повідомлення надійшло від людини, яку ви знаєте. (2 бали)
4) Ви наводите курсор миші на посилання, щоб перевірити кінцеву URL адресу перед тим як натиснути. (1 бал)

d. Під час відвідування веб-сайту відображається спливаюче вікно. У ньому говориться, що ваш комп'ютер знаходиться під загрозою, і ви повинні завантажити та встановити діагностичну програму, щоб захистити свій комп'ютер: _____

1) Ви натискаєте, завантажуєте та встановлюєте програму, щоб захистити ваш комп'ютер. (3 бали)
2) Ви перевіряєте спливаючі вікна та наводите курсор на посилання, щоб перевірити його безпечність. (3 бали)
3) Ігноруєте повідомлення, переконавшись, що ви не натиснули на нього, не завантажуєте програму та закриваєте веб-сайт. (0 балів)

e. Коли вам потрібно увійти на веб-сайт своєї фінансової установи, щоб виконати щось, ви: _____

1) Вводите свою реєстраційну інформацію негайно. (3 бали)
2) Ви перевіряєте URL, щоб переконатися, що це заклад, який вам потрібен, перед введенням будь-якої інформації. (0 балів)
3) Ви не використовуєте онлайн-банкінг або будь-які онлайн-фінансові послуги. (0 балів)

f. Ви прочитали про програму і вирішили спробувати її. Ви шукаєте в Інтернеті та знаходите пробну версію на невідомому сайті, ви: _____

1) Негайно завантажуєте та встановлюєте програму. (3 бали)
2) Шукаєте більше інформації про автора програми, перш ніж завантажувати її. (1 бал)
3) Не завантажуєте та не встановлюєте програму. (0 балів)

g. Ви знаходите USB-диск на шляху до роботи, ви: _____

1) Берете його та підключаєте до комп'ютера, щоб переглянути його вміст. (3 бали)
2) Берете його та підключаєте до комп'ютера, щоб стерти його вміст перед використанням. (3 бали)
3) Берете його та підключаєте до комп'ютера, щоб запустити антивірусне сканування, перш ніж повторно використовувати його для власних файлів (3 бали)
4) Не піднімаєте його. (0 балів)

h. Вам потрібно підключитися до Інтернету і ви знаходите відкриту точку доступу Wi-Fi. Ви: _____

1) Підключаєтеся до неї та користуєтесь Інтернетом. (3 бали)
2) Не підключаєтеся до неї та чекаєте на появу надійного з'єднання з Інтернетом. (0 балів)
3) Підключаєтеся до неї та встановлюєте VPN з’єднання з надійним сервером перед надсиланням будь-якої інформації. (0 балів)

Частина 2: Проаналізуйте свою поведінку в Інтернеті

Чим більша ваша сума балів, тим менш безпечною є ваша поведінка в Інтернеті. Вашою метою має бути 100% безпека, якої ви зможете досягнути, звертаючи увагу на всі свої дії онлайн. Це дуже важливо, оскільки навіть одна помилка може поставити під загрозу ваш комп'ютер та дані.

Просумуйте бали, набрані в Частини 1. Запишіть свою суму балів. _____

0: Ви дуже безпечно поводите себе в Інтернеті.

0-3: Ви частково безпечно поводите себе в Інтернеті, але все одно повинні трохи змінити свою поведінку, щоб вона була повністю безпечною.

4-17: Ваша поведінка у Інтернеті небезпечна і ви ризикуєте поставити себе під загрозу.

18 або більше: Ваша поведінка в Інтернеті дуже небезпечна і ваші дані будуть скомпрометовані.

Нижче наведено кілька важливих порад щодо безпеки в Інтернеті.

a. Чим більшою кількістю інформації ви ділитеся в соціальних мережах, тим більше ви дозволяєте зловмисникові дізнатися про вас. Маючи більше знань про вас, зловмисник може створити набагато більш спрямовану атаку. Наприклад, якщо ви поділитеся зі світом інформацією про те, що ви були на автомобільних перегонах, зловмисник зможе надіслати вам електронного листа від імені компанії, яка відповідальна за продажу квитків на перегони. Оскільки ви нещодавно були на цьому заході, повідомлення буде виглядати надійним.

b. Повторне використання паролів − це погана практика. Якщо ви повторно використовуєте пароль у службі, що знаходиться під контролем зловмисників, вони можуть спробувати успішно увійти під вашим обліковим записом у інші служби.

c. Електронні листи можна легко підробити, щоб вони виглядали надійно. Підроблені електронні листи часто містять посилання на шкідливі сайти або шкідливе програмне забезпечення. Візьміть за правило не натискати на вкладенні посилання з листів, отриманих електронною поштою.

d. Не погоджуйтесь на встановлення небажаного програмного забезпечення, особливо якщо його пропонують вам на веб-сторінці. Дуже малоймовірно, що ця веб-сторінка пропонувала вам легальне та безпечне програмне забезпечення. Настійно рекомендується закрити браузер та використати інструменти операційної системи, щоб перевірити наявність оновлень.

e. Шкідливі веб-сторінки легко можна зробити схожими на веб-сайт банку або фінансової установи. Перш ніж натискати посилання або надавати будь-яку інформацію, двічі перевірте URL-адресу, щоб переконатися, що це правильна веб-сторінка.

f. Коли ви дозволяєте програмі запускатись на вашому комп'ютері, ви даєте їй багато можливостей. Добре подумайте перш ніж запускати програму. Проведіть невелике дослідження, щоб переконатися, що компанія або особа, відповідальна за програму, є серйозним та законним автором. Завантажуйте цю програму лише з офіційного веб-сайту компанії чи особи.

g. USB-накопичувачі та флешки містять мініатюрний контролер, що дозволяє комп'ютерам з ними спілкуватися. Цей контролер можна заразити і навчити встановлювати шкідливе програмне забезпечення на комп'ютер. Оскільки шкідливе програмне забезпечення розміщується безпосередньо в контролері USB, а не в області даних, то видалення даних або антивірусне сканування не виявить зловмисне програмне забезпечення.

h. Зловмисники часто розгортають підроблені точки доступу Wi-Fi, щоб заманити користувачів. Оскільки атакуючий має доступ до всієї інформації, переданої через скомпрометовану точку доступу, користувачі, підключені до цієї точки доступу, піддаються ризику. Ніколи не використовуйте невідомі точки Wi-Fi, не шифруючи трафік через VPN. Ніколи не передавайте конфіденційні дані, такі як номери кредитних карток, під час використання невідомої мережі (дротової або бездротової).

Дайте відповідь на запитання

Проаналізувавши свою поведінку в Інтернеті, які зміни ви б зробили, щоб захистити себе?

_____

_____

_____

_____