Чи захищені ваші електронні файли і почта?

Мета: Вивчити що таке пароль, а також навчитися створювати надійні паролі для захисту комп'ютерної інформації і особистих файлів.

Що таке пароль?

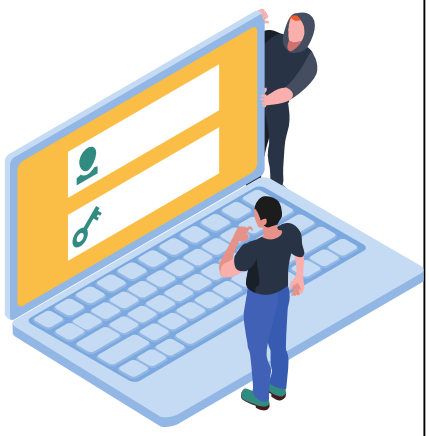
Значення: **Пароль**
це особисто вибраний таємний шифрований рядок із літер, цифр і спеціальних символів, який використовується для відкритя файлів або для авторизації доступу до комп'ютерних даних.

Що робить пароль надійним і чому це важливо?

Надійний пароль – це пароль, який відомий лише власнику електронної почти і навряд чи його вгадає хтось інший. Щоб зробити пароль складним і електронно безпечним, додаються спеціальні символи, великі літери або цифри. Дуже важливо мати надійний складний пароль до комп'ютера, оскільки він підвищує безпеку ваших особистих файлів, репутації та конфіденційної інформації.

Activity

1. Think about the complexity of the passwords for your various sites and accounts.
2. Explore the Password Strength Meter by visiting: www.passwordmonster.com
3. Make up a few passwords to test... you can even test your current one.
4. Discuss with others why it is important to have a strong password.
5. Consider updating your passwords to increase their security.



Наскільки складний ваш пароль? Чи зможуть ваш пароль розгадати? Який найнадійніший і найскладніший пароль ви можете запам'ятати? Як довго ви його придумували?

KENT SCHOOL DISTRICT
EQUITY | EXCELLENCE | COMMUNITY

Складнощі фішингу

Мета: Зрозуміти що таке фішинг і визначати різні особливості фішингу.

Що таке фішинг?

Значення: **Фішинг**

це цифрова форма соціальної електронної інженерії, яка використовує і висилає правдоподібні, але фальшиві електронні листи, для того, щоб отримати конфіденційну інформацію від користувачів аби спрямувати їх на фальшивий веб-сайт, який запитує і колекціонує персональну інформацію.

Як розпізнати фішинговий електронний лист?

- Чи знаєте ви відправника? Це той, від кого ви очікували повідомлення, або з ким ви спілкуєтеся постійно?
- Обов'язково перевірте на наявність помилок в повідомленні чи лінку, перш ніж натискати на них.
- Зверніть увагу на вітання, від кого та підпис.
- Чи здається вам, що це повідомлення є недоречне? Як що так, то будьте обережні. Довіряйте своїй інтуїції та не натискайте на посилання, чи лінк і не відповідайте відправнику. Зразу видаліть цей імейл.

Попрактикуйте:

1. Поміркуйте, як розпізнати фішингове шахрайство.
2. Скориставшись наведеними вище порадами, чи зможете ви визначити три індикатори фішингу в електронному листі на наступній сторінці.
3. Поділіться з іншими, як і чому потрібно остерігатися фішингу та не потрапити на гачок до шахраїв.

Чи знаєте ви, що після того, як ви виявили фішинговий електронний лист, розумно видалити його зразу, щоб потім не повертатися до нього?

Складнощі фішингу

Попрактикуйте: Завдання - знайти ознаки фішінгу в імейлі

Hello You Have New Vmail

SN

stuart.fletcher New-Call <sf@prizemons.com>

To Name, Your

Reply | Reply All | Forward

Fri 9/29/2023 2:26 PM

Follow up. Completed on Friday, September 29, 2023.

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Outlook

Hello,

You have new voicemail message in your mailbox.

This mail was sent to: Your.Name@kent.k12.wa.us

Preview or Download Voice Message

Sincerely,

Microsoft Customer Care

Microsoft | Support | Privacy Policy

Copyright © 2020 Microsoft .Inc

Microsoft Outlook WebApp

OWA

Відповідь: Top 3 issues

From: stuart.fletcher New-Call <sf@prizemons.com>

Назва відправника імейла недоречна і прихове відправника та електронну пошту для відповіді.

Hello,

Граматичні помилки, помилки в прізвищі та імені.

Sincerely,

Microsoft Customer Care

Повідомлення містить мало відомостей про відправника, його контактну інформацію та ім'я адміна.

Що таке багатофакторна автентифікація (MFA)?

Мета: Дізнатися, що таке багатофакторна автентифікація (MFA) та вміти визначати елементи, які можуть бути використані для багатофакторної автентифікації.

Що таке багатофакторна автентифікація

Визначення: Багатофакторна автентифікація Поєднання чогось, чого ви є власником (речі); чогось, що ви пам'ятаєте (зберігається в вашій пам'яті, як ваші особисті таємниці); або щось, що описує вас, як особистість (професія, менталітет, харектеристика). Зазвичай, використовується для розпізнання особи щоб захистити ваші ресурси (фізичне місцезнаходження, дані, кошти).

Що можуть бути предметами MFA?

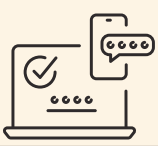
- Річ + подія, яку ви пам'ятаєте + фізична карта доступу + PIN-код.
- Ваша характеристика + подія, яку ви пам'ятаєте + біометрія обличчя + PIN-код.
- Ваша характеристика + річ + фізична карта доступу + сканування сітківки ока.

Попрактикуйте

Чи можете ви визначити різні комбінації MFA? Напишіть ваші відповіді після кожної фрази словом - Вірно, коли вірна відповідь і словом - Невірно - коли фраза не описує MFA.

1. Картка банкомату та PIN-код ..... В-Вірно/Н-Невірно
2. Відбиток пальця та розпізнавання обличчя ..... В-Вірно/Н-Невірно
3. Карточка посвідчення і пароль ..... В-Вірно/Н-Невірно
4. Розпізнавання обличчя і пін-код ..... В-Вірно/Н-Невірно
5. Особисті запитання та ім'я користувача..... В-Вірно/Н-Невірно
6. Електронна пошта та пароль ..... В-Вірно/Н-Невірно
7. Пароль і PIN-код ..... В-Вірно/Н-Невірно
8. Флеш-память або Key Fob, код доступу та сканування відбитків пальців ..... В-Вірно/Н-Невірно

Відповіді до запитань: 1-В 2-Н 3-В 4-В 5-Н 6-Н 7-Н 8-В



Які ви маєте електронні пристрої і банківські сервіси, де використовуєте багатофакторну автентифікацію? Поділіться, як MFA може захистити вашу особисту інформацію.

Зашифрований і не зашифрований вебсайт

Мета: Дізнатися, що таке шифрування веб-сайтів, і вміти визначити, чи є веб-сайт зашифрований.

Що таке шифрування сайту?

Визначення: Шифрування веб-сайту
HTTPS (Hypertext Transfer Protocol Secure) – це один із видів безпеки і захисту ваших повідомлень під час спілкування з веб-сайтом. Це як, таємний код, який зберігає ваші слова і інформацію в безпеці. Коли ви надсилаєте повідомлення на веб-сайті, то для їх захисту вони перетворюються на таємний код. І коли веб-сайт зв'язується з вами, він також використовує таємний код для забезпечення безпеки своєї інформації.

Як дізнатися, що ваш сайт зашифровано?

Ви можете визначити, чи використовує веб-сайт HTTPS, подивившись на крихітний замок в адресному рядку у верхній частині екрана компютера, ліворуч від назви веб-сайту. Якщо ви бачите замок, це означає, що ваші повідомлення в безпеці. Але якщо замка немає або якщо замок має червону лінію, це означає, що ваші повідомлення в небезпеці вони є незахищені, тому будьте обережні!

Пропонуємо ігру:

Полювання або Знаходження Зашифрованих і Не Зашифрованих Вебсайтів. Перевірте, чи є ваші улюблені електронні сайти безпечними для вашого комп'ютера. Знайдіть час, щоб перевірити нижче поданні приклади вебсайтів. Перевірте, які з них зашифровані або мають замочок, що є безпечним для відвідування їх, а які не мають замок, що означає ці сайти не захищенні. Напишіть Так, коли є замочок і Ні – коли його не має.

- [ ] На улюблених соціальних сайтах
- [ ] На улюбленому ігровому сайті
- [ ] На вашій онлайн почті в Інтернеті
- [ ] На сайті онлайн-навчання
- [ ] На улюбленому веб-сайті для кінофільмів і соціальних програм
- [ ] На улюбленій пошуковій системі

Чи ви знайшли вебсайти, які часто відвідуєте, але вони не були зашифровані (не мали значка ключика)? Поділіться з іншими, чому важливо перед тим, як відкрити вебсайт треба знати чи він зашифрований (має помітку - замочка)?

Електрона Соціальна Інженерія (Спам)

Мета: Дізнатися, що таке соціальна інженерія (спам), і вміти визначати основні риси спамових атак на ваш компютер.

Що таке соціальна інженерія?

Визначення: **соціальна інженерія**
Використання маніпуляційних тактик, щоб обманом змусити людину розкрити свою конфіденційну інформацію, отримати несанкціонований доступ до комп'ютерних файлів і вчинити шахрайство. Хакери обманним шляхом використовувають ваші почту і імейл. Вони від вашого імені збрають потрібну їм інформацію, а також дискредитують вашу репутацію і довіру до вас з боку вашої організації.

Які риси притаманні нападу соціальної інженерії?

Спамери полюють на ваше мислення та емоції. Маніпулятивні риси соціального інженера або спамера:

1. **Зіграти на ваших підвищених емоціях:** ви з більшою ймовірністю зробите ірраціональний або ризикований вибір, коли будете в емоційному стані (злість, страх, збудження тощо).
2. **Терміновість:** Їхні дії або слова будуть сформульовані таким чином, щоб змусити вас відчути, що ви повинні прийняти негайно необґрунтоване рішення нав'язане ними.
3. **Довіра:** Вони намагатимуться виглядати як надійне джерело або вірний друг.

Попрактикуйте

Чи можете ви визначити, яку маніпулятивну рису використовують наступні приклади атак соціальної інженерії? Позначте кожну рису номером
1 - Емоції, 2 - Терміновість, 3 - Довіра

_____ Повідомлення з невідомого номера про те, що посилка загублена і їм потрібна повторно ваша конфедиціальна інформація, щоб підтвердити відправку іншої.

_____ Спливаюче вікно в Інтернеті про те, що ви виграли приз, який трапляється раз у житті, але повинні подати заявку протягом 15 хвилин, заповнивши деяку особисту інформацію.

_____ Ви бачите спливаюче вікно в Інтернеті з попередженням про те, що ваш комп'ютер заражено, і щоб виправити це, ви повинні завантажити спеціальне програмне забезпечення для захисту від зловмисної та шкідливої програми.

_____ Ваш найкращий друг надсилає вам електронний лист із проханням переглянути дивний лінк, який веде вас до фотографій з нещодавньої подорожі.

Ключ до відповідей: 1, 3, 2, 3

Чи можете ви уявити собі атаку соціальної інженерії (спам), яка використовує всі три риси? Поділіться з іншими, як ви можете підготуватися до атак соціальної інженерії (спаму) та уникнути їх?