1. **Яка з наведених загроз є найбільш поширеною при використанні незахищених мереж Wi-Fi для роботи з корпоративною поштою?**

А) Фішинг

Б) Віруси

В) DDoS-атаки

Г) Всі перелічені

1. **Який з наведених способів є найбільш ефективним для захисту паролів від злому?**

А) Використання простих, легко запам'ятовуваних паролів

Б) Використання одного пароля для всіх облікових записів

В) Використання складних, унікальних паролів для кожного облікового запису

Г) Запис паролів на папері

1. **Що таке фішинг?**

А) Несанкціонований доступ до комп'ютерної системи

Б) Спроба отримати конфіденційну інформацію шляхом обману

В) Розповсюдження шкідливого програмного забезпечення

Г) Відмова у обслуговуванні сервісу

1. **Які дані вважаються конфіденційними в більшості організацій?**

А) Номери телефонів співробітників

Б) Банківські реквізити клієнтів

В) Графіки відпусток

Г) Всі перелічені

1. **Який з наведених заходів не є ефективним для захисту від вірусів?**

А) Регулярне оновлення антивірусного програмного забезпечення

Б) Відкриття всіх вкладених файлів в електронних листах

В) Уважне ставлення до підозрілих посилань

Г) Створення резервних копій даних

1. **Що таке двофакторна аутентифікація?**

А) Введення пароля двічі

Б) Використання пароля та додаткового засобу аутентифікації (наприклад, коду з SMS)

В) Підтвердження особи за допомогою відбитків пальців

Г) Введення пароля і логіна

1. **Як правильно утилізувати носії інформації, що містять конфіденційні дані?**

А) Викинути в звичайний смітник

Б) Відформатувати і використовувати повторно

В) Знищити фізично (наприклад, подрібнити)

Г) Зберегти на випадок, якщо знадобляться дані

1. **Які ризики пов'язані з використанням особистих пристроїв для роботи?**

А) Ризик зараження вірусами

Б) Ризик втрати даних

В) Ризик несанкціонованого доступу до корпоративної мережі

Г) Всі перелічені

1. **Яка з наведених дій є найбільш небезпечною при роботі в організаційній соціальній мережі?**

А) Обмін досвідом з колегами

Б) Публікація особистої інформації

В) Обговорення робочих питань

Г) Використання корпоративної пошти для спілкування

1. **Що таке фішинг в контексті соціальних мереж?**

А) Створення фейкових профілів для збору інформації

Б) Розповсюдження шкідливого програмного забезпечення

В) Несанкціонований доступ до облікового запису

Г) Всі перелічені варіанти

1. **Яку інформацію не слід публікувати в організаційній соціальній мережі?**

А) Інформацію про відпустку

Б) Контактні дані колег

В) Результати проектів

Г) Всі перелічені варіанти

1. **Як захистити свій обліковий запис в організаційній соціальній мережі?**

А) Використовувати простий пароль

Б) Не включати двофакторну аутентифікацію

В) Регулярно змінювати пароль

Г) Поділитися паролем з колегами

1. **Що таке соціальна інженерія в контексті соціальних мереж?**

А) Використання технічних засобів для отримання доступу до інформації

Б) Маніпуляція людьми для отримання конфіденційної інформації

В) Розповсюдження шкідливого програмного забезпечення

Г) Несанкціонований доступ до серверів

1. **Які ризики пов'язані з використанням особистих пристроїв для доступу до організаційної соціальної мережі?**

А) Ризик зараження вірусами

Б) Ризик втрати даних

В) Ризик несанкціонованого доступу до корпоративної мережі

Г) Всі перелічені варіанти

1. **Як правильно реагувати на підозрілі повідомлення в організаційній соціальній мережі?**

А) Відповісти на повідомлення

Б) Перейти за посиланням, вказаним у повідомленні

В) Ігнорувати повідомлення та повідомити адміністратора

Г) Поділитися повідомленням з іншими користувачами

1. **Які заходи безпеки слід вживати при роботі з документами, які розміщені в організаційній соціальній мережі?**

А) Перевіряти документи на наявність вірусів перед завантаженням

Б) Обмежити доступ до документів тільки для авторизованих користувачів

В) Регулярно створювати резервні копії документів

Г) Всі перелічені варіанти

1. **Що таке фішинг?**

А) Несанкціонований доступ до комп’ютерної системи

Б) Спроба отримати конфіденційну інформацію шляхом обману

В) Розповсюдження шкідливого програмного забезпечення

Г) Відмова у обслуговуванні сервісу

1. **Який з наведених способів є найчастіше використовуваним для фішингу?**

А) Дзвінки по телефону

Б) Фішингові електронні листи

В) СМС-повідомлення

Г) Всі перелічені варіанти

1. **Які дані найчастіше намагаються виманити фішери?**

А) Номери телефонів

Б) Логіни та паролі

В) Номери кредитних карток

Г) Всі перелічені варіанти

1. **Як правило, фішингові електронні листи містять:**

А) Посилання на офіційні сайти

Б) Повідомлення про виграш у лотереї

В) Помилки в граматиці та орфографії

Г) Всі перелічені варіанти

1. **Які ознаки можуть вказувати на фішингове повідомлення?**

А) Незвичний відправник

Б) Посилання на невідомі сайти

В) Повідомлення про термінову дію

Г) Всі перелічені варіанти

1. **Що слід робити, якщо ви отримали підозрілий електронний лист?**

А) Відповісти на лист

Б) Перейти за посиланням, вказаним у листі

В) Видалити лист, не відкриваючи його

Г) Переслати лист усім контактам

1. **Як захистити себе від фішингу?**

А) Використовувати складні паролі

Б) Не відкривати підозрілі вкладення

В) Бути обережним при переході за посиланнями

Г) Всі перелічені варіанти

1. **Яку роль відіграє людський фактор у фішингових атаках?**

А) Незначна

Б) Дуже велика

В) Залежить від типу атаки

Г) Немає правильної відповіді