



Завдання та відповіді для педагога для гри «Правда чи фейк»

Блок 1. Паролі та двофакторна автентифікація.

Твердження № 1

Пароль «123456» можна зламати лише за одну секунду.

Відповідь для педагога: ☒ правда. Такий пароль найпоширеніший. За даними розробників менеджера паролів “NordPass”, цю комбінацію у 2024 році використали понад три мільйони разів.

Твердження № 2

Використовувати один і той самий пароль для кількох акаунтів — це безпечно.

Відповідь для педагога: ☐ фейк. Це небезпечно, бо зламавши один акаунт, шахрай зможе отримати доступ до всіх інших.

Твердження № 3

Пароль з іменем домашнього улюбленця — це надійний варіант пароля.

Відповідь для педагога: ☐ фейк. Така інформація може бути легкодоступною в соціальних мережах чи інших джерелах.

Твердження № 4

Надійний пароль має складатися щонайменше з 12 символів.

Відповідь для педагога: ☒ правда. Чим довший пароль, тим складніше його зламати.

Твердження № 5

Записувати пароль у нотатках на телефоні — це надійний спосіб його зберегти.

Відповідь для педагога: ☐ фейк. Це як зберігати золото в пакеті із супермаркету. Ліпше — менеджер паролів.

Твердження № 6

Надійний пароль можна створити на основі фрази, яка вам близька, наприклад, абсурдний факт про себе.

Відповідь для педагога: ☒ правда. Це простий і дієвий лайфхак, бо пароль має особистий сенс, але складний для зламу.

Твердження № 7

Паролі в браузері зберігати безпечно, бо сучасні браузери шифрують дані.

Відповідь для педагога: ✗ фейк. У разі зламу пристрою всі паролі опиняться в руках шахрая.

Твердження № 8

Двофакторна автентифікація захищає акаунт навіть у разі викрадення пароля.

Відповідь для педагога: ✓ правда. Шахрай без додаткового коду не зможе увійти.

Твердження № 9

Резервні коди — це запасний спосіб входу в акаунт, якщо немає доступу до телефону.

Відповідь для педагога: ✓ правда. Їх варто зберігати в надійному місці, але не в нотатках телефону.

Твердження № 10

Брутфорс — це атака групою людей, які вручну перебирають паролі.

Відповідь для педагога: ✗ фейк. Це автоматизований процес, який здійснює програма, а не людина.

Блок 2. Секретні запитання.

Секретні запитання — це запитання, які з'являються, коли тиснете “Забув(ла) пароль?”. Відповіли правильно — акаунт знову ваш. Такі запитання та відповідь ви обираєте самостійно під час налаштування акаунту.

Твердження № 11

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: скільки буде 2+2?

Відповідь: 67алеценеточно.

Відповідь для педагога: ✓ правда. Це вигадана відповідь, яку неможливо вгадати чи знайти інформацію у відкритих джерелах.

Твердження № 12

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: яке ім'я мого kota?

Відповідь: Джек.

Відповідь для педагога: ✓ фейк. Це ризиковано, ім'я домашнього улюбленця часто доступне в профілях / публікаціях.

Твердження № 13

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: яка назва моєї вигаданої планети?

Відповідь: ZorgonBlue_42

Відповідь для педагога: ☒ правда. Це вигадана відповідь, приватна, незвична інформація; така пара (запитання+незвична відповідь) надійна для захисту акаунту.

Твердження № 14

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: у якому місті я народився?

Відповідь: Kyiv

Відповідь для педагога: ☐ фейк. Місце народження — часто публічна інформація.

Твердження № 15

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: яке кодове слово я вигадав сам?

Відповідь: КвіткаСіріус_#9

Відповідь для педагога: ☒ правда. Кодове слово, самостійно вигадане, є приватним та унікальним, що підвищує безпеку.

Твердження № 16

Таке секретне запитання та відповідь є надійними для захисту акаунту.

Запитання: Як звали мого першого вчителя?

Відповідь: Olena

Відповідь для педагога: ☐ фейк. Ім'я першого вчителя — часто відоме або його можна легко знайти.

Блок 3. Злам акаунтів.

Твердження № 17

Логотип відомого бренду гарантує, що сайт або сторінка — справжні.

Відповідь для педагога: ☐ фейк. Шахраї копіюють логотипи й дизайн сайтів відомих брендів, щоб видати фейк за правду — перевіряйте сайт та інформацію через офіційні джерела.

Твердження № 18

Після того, як акаунт зламано, шахраї зазвичай одразу пишуть від імені власника акаунту іншим людям.

Відповідь для педагога: ☒ правда. Це класична схема — розсилка фішингових посилань від чужого імені.

Твердження № 19

Якщо в SMS / повідомленні в месенджері йдеться про виклик до суду із посиланням — одразу треба перейти і перевірити деталі.

Відповідь для педагога: ✗ фейк. Посилання з таких SMS чи повідомлень часто ведуть на фейкові сайти. Перевіряйте інформацію через офіційні джерела, не переходьте за підозрілими посиланнями.

Твердження № 20

Meta (Instagram / Facebook) пише в Direct про блокування акаунту та просить ввести логін / пароль, перейшовши за посиланням, щоб ви могли запобігти блокуванню.

Відповідь для педагога: ✗ фейк. Справжня Meta не надсилає такі вимоги через Direct; офіційні листи можна знайти в налаштуваннях «Нещодавні електронні листи».

Твердження № 21

Якщо ви ввели пароль від акаунту в соціальних мережах на шахрайському сайті, але ще маєте доступ до акаунту — треба перевірити активні сесии та завершити підозрілі, а потім змінити пароль до акаунту.

Відповідь для педагога: ✓ правда. Це допоможе припинити чужий доступ і швидко змінити пароль.

Твердження № 22

Увімкнути сповіщення про підозрілий вхід — корисно, бо це дає змогу швидко дізнатися про несанкціонований доступ.

Відповідь: ✓ правда. Такі сповіщення інформують про нові пристрої / локації входу, їх слід увімкнути.

Твердження № 23

Якщо друг в соціальній мережі просить позичити гроші і надсилає голосове повідомлення з проханням — краще одразу переказати.

Відповідь для педагога: ✗ фейк. Шахраї зламують акаунти та від імені їх власників пишуть друзям і підписникам. Перш ніж переказати гроші, зателефонуйте або задайте питання, на яке знає відповідь тільки друг та ви.

Твердження № 24

Не переходьте за посиланнями навіть від друзів, бо їх акаунти можуть бути зламани.

Відповідь: ✓ правда. Якщо друг надсилає посилання, перш ніж натискати, уточніть по телефону, чи це дійсно пише він, а не шахрай.

Твердження № 25

Попросити ввести логін і пароль від сторінки у Facebook для підпису петиції — нормальна практика.

Відповідь: ✗ фейк. Справжній процес підпису відбувається на офіційному сайті й через офіційні способи ідентифікації BankID / ЕЦП.