Кібербезпека та протидія шахрайству при роботі в Інтернет та з електронною поштою

Бєгун Сергій Васильович,
с.н.с. відділу освітньо-наукової діяльності,
кандидат фізико-математичних наук

План лекції

1. Чому це важливо: ситуація 2026 року (5 хв)
2. Основні загрози: фішинг, соціальна інженерія, ransomware (7 хв)
3. Розпізнавання фішингових листів — практикум (8 хв)
4. Безпечна робота з е-поштою, посиланнями та вкладеннями (5 хв)
5. Парольна політика та двофакторна автентифікація (7 хв)
6. Робоче місце, змінні носії та штучний інтелект (5 хв)
7. Дії у разі виявлення кіберзагрози (5 хв)
8. Підсумки та контрольні питання (3 хв)

РОЗДІЛ 1. ЧОМУ ЦЕ ВАЖЛИВО: СИТУАЦІЯ 2026 РОКУ

Лист НАМН України (квітень 2026)

- МОЗ та НАМН провели контрольовану імітацію цілеспрямованої кібератаки
- Метод: соціальна інженерія — фішингові листи на офіційні адреси установ
- Тема-приманка: «необхідність оновлення та верифікації доступу до СЕД»
- Мета: оцінити алгоритм дій персоналу при отриманні підозрілих листів
- Результат: працівники низки установ:

    1) зайшли на підготовлені «фішинг» сайти;

    2) ввели паролі на цих «фішинг» сайтах, включаючи РЕАЛЬНІ паролі доступу.

- Висновок: компрометація автентифікаційних даних → ризик доступу до внутрішніх систем, витоку документації, поширення шкідливого ПЗ (Ransomware) у мережі установи

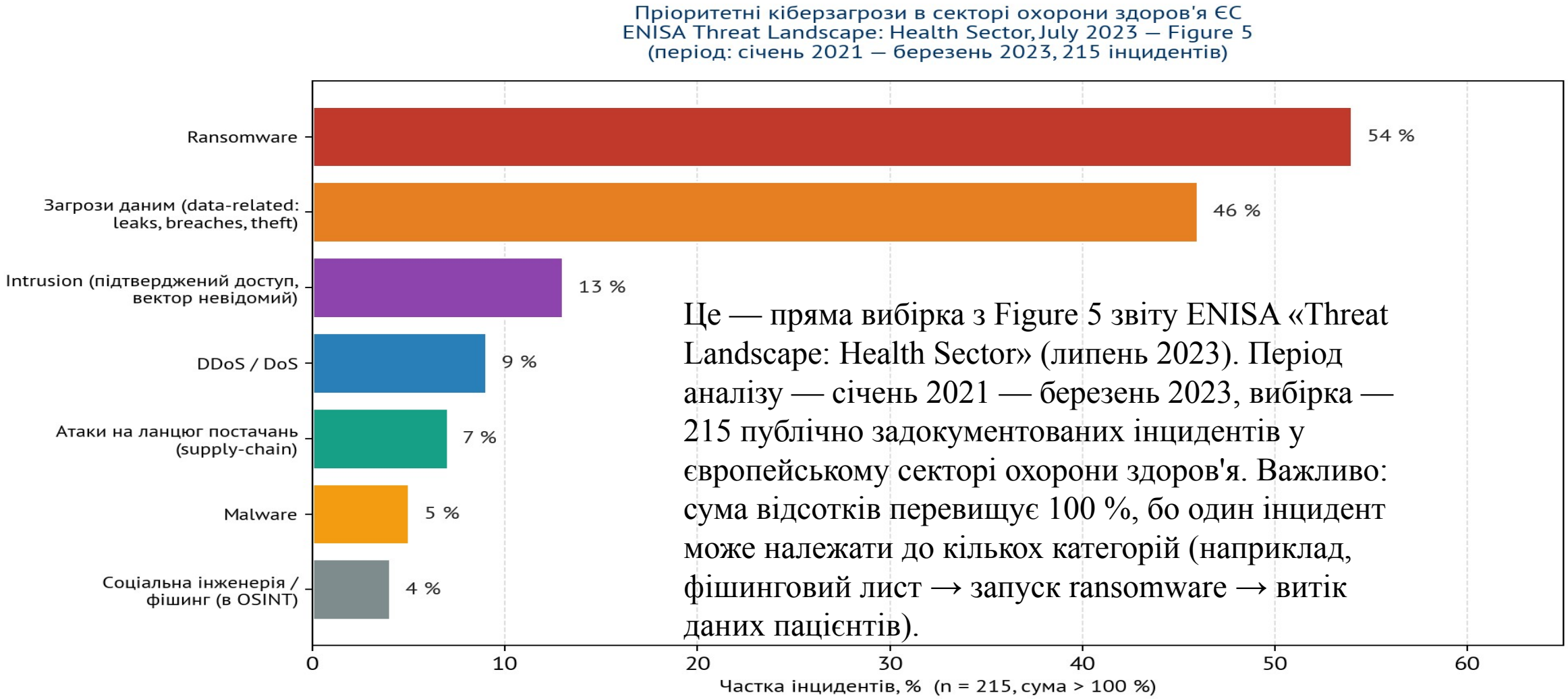
Чому медичні заклади та наукові установи можуть бути пріоритетною ціллю атак

- **Чутливі персональні дані пацієнтів — високооплачуваний товар у даркнеті**
- **Критичність роботи — потенційний доступ зловмисників до критично важливих технологічних даних чи обладнання – іноді установа готова заплатити викуп, щоб відновити доступ**
- **Велика поверхня атаки: лікарі, медсестри, науковці, допоміжний персонал, адміністрація, бухгалтерія**
- **Часто застарілі інформаційні системи та брак IT-персоналу**
- **Цілеспрямовані APT-групи розповсюджують шкідливе ПЗ під виглядом у тому числі гуманітарних ініціатив**

(APT-групи (від англ. Advanced Persistent Threat — розвинена стійка загроза) — це висококваліфіковані угруповання кіберзлочинців, діяльність яких зазвичай спонсорується на рівні держав. Вони здійснюють довготривалі та приховані кібератаки для розвідки, шпигунства або завдання критичної шкоди.)

- **В умовах війни — додатковий політично мотивований інтерес противника**

Пріоритетні кіберзагрози в охороні здоров'я ЄС (ENISA, 2023)



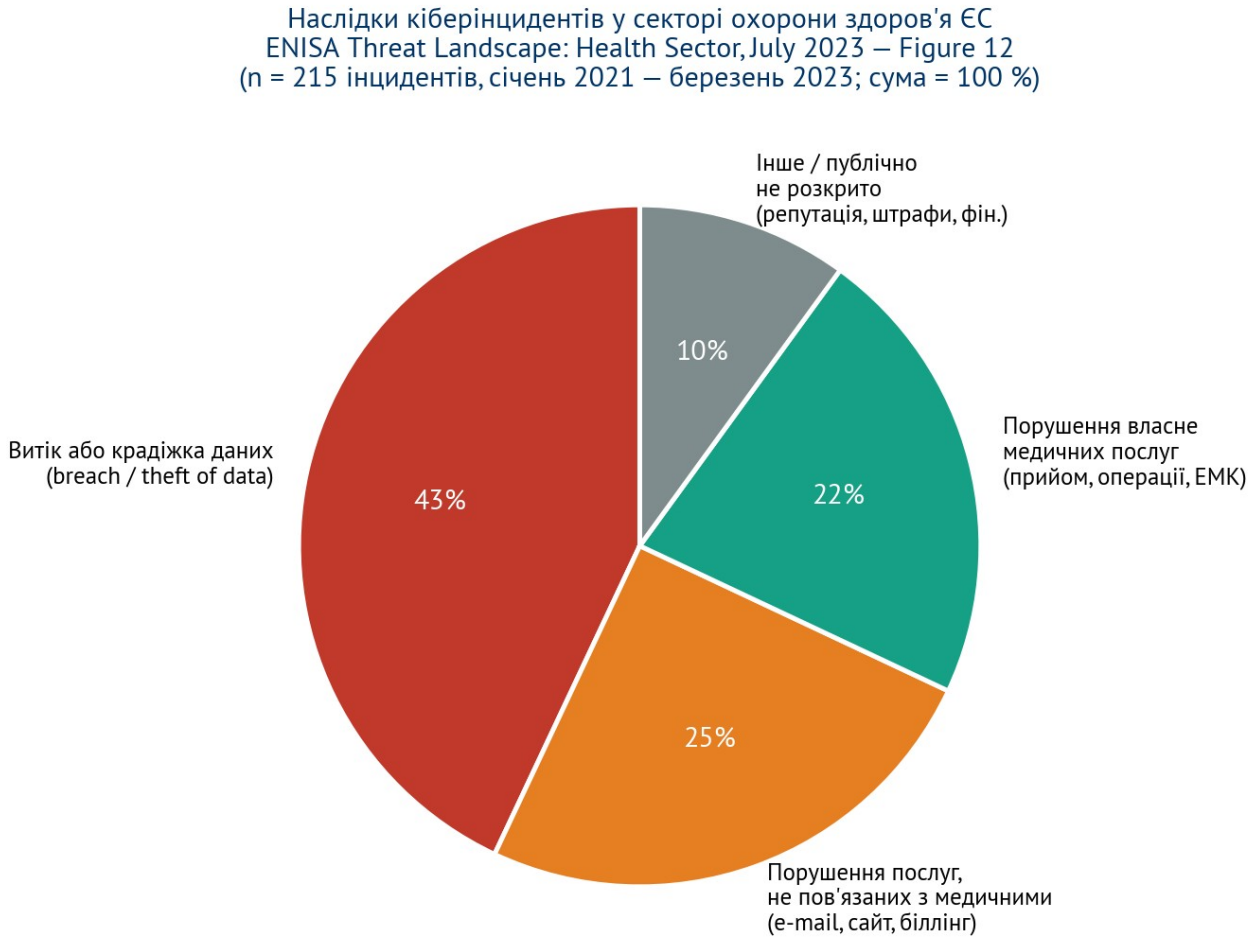
Це — пряма вибірка з Figure 5 звіту ENISA «Threat Landscape: Health Sector» (липень 2023). Період аналізу — січень 2021 — березень 2023, вибірка — 215 публічно задокументованих інцидентів у європейському секторі охорони здоров'я. Важливо: сума відсотків перевищує 100 %, бо один інцидент може належати до кількох категорій (наприклад, фішинговий лист → запуск ransomware → витік даних пацієнтів).

Джерело: ENISA, «Threat Landscape: Health Sector», July 2023, Figure 5 (с. 11), n = 215 інцидентів, січень 2021 — березень 2023.
PDF: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

Структура кіберінцидентів в охороні здоров'я

- На першому місці — ransomware: шифрувальники задіяні у 54 % інцидентів, і в 43 % випадків вони супроводжуються крадіжкою даних.
- Майже паритетна частка — 46 % — загрози саме даним: витоки, продаж в даркнеті, розкриття медичних карток.
- 13 % — «intrusion», тобто підтверджений несанкціонований доступ, при якому публічно невідомо, як саме відбувся вхід у систему.
- 9 % — DDoS-атаки (суттєве зростання у початку 2023 року через проросійський хактивізм).
- 7 % — атаки на ланцюг постачань (supply-chain).
- 5 % — malware.
- Соціальна інженерія як окрема категорія — лише ~4 %, але це явне заниження: ENISA прямо вказує, що в 95 % інцидентів первинний вектор доступу публічно не розкривається, а відомо, що саме фішинг є основним способом проникнення у більшості ransomware-кампаній. Отже реальна частка атак, що починаються з листа людині, значно вища за ці 4 %.
- Висновок для працівника: ваш поштовий клік — це потенційний перший крок саме тієї 54 %-ої ransomware-атаки, що потім зафіксується у статистиці європейського агентства з кібербезпеки.

Наслідки кіберінцидентів в охороні здоров'я ЄС (ENISA, 2023)



Джерело: ENISA, «Threat Landscape: Health Sector», July 2023, Figure 12 (с. 26), n = 215 інцидентів, січень 2021 — березень 2023. PDF: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

РОЗДІЛ 2. ОСНОВНІ ЗАГРОЗИ ТА ПОНЯТТЯ

Соціальна інженерія — головний інструмент зловмисника

Соціальна інженерія — це маніпулювання людиною з метою змусити їїмвчинити дію, що дає зловмиснику доступ до інформації чи систем.

Універсальні «гачки», які експлуатуються:

- **Авторитет — лист «від керівника», «від ІТ-відділу», «від МОЗ»**
- **Терміновість і страх — «протягом 24 годин буде заблоковано»**
- **Цікавість — «Ваша зарплатна відомість у вкладенні»**
- **Вигода — «Вам нараховано надбавку, підтвердіть реквізити»**
- **Довіра — лист нібито від відомого колеги (зламана пошта)**

Фішинг та його різновиди

Фішинг (phishing) — масове розсилання листів-приманок з метою змусити одержувача перейти на підроблений сайт або відкрити шкідливий файл.

Цільові різновиди:

- **Spear phishing — точкова атака на конкретну людину (наприклад, головбух)**
- **Whaling — «полювання на кита»: атака на топ-керівництво**
- **BEC (Business Email Compromise) — підробка ділового листування**
- **Vishing — фішинг по телефону (Voice phishing)**
- **Smishing — фішинг через SMS / Viber / Telegram**
- **QRishing — підроблені QR-коди (на афішах, у листах, на паркуваннях)**

Ransomware — шифрувальники

Ransomware — шкідливе ПЗ, що шифрує файли на комп'ютері і всій мережі,

а потім вимагає викуп за розшифрування (зазвичай у криптовалюті).

Як потрапляє в мережу медичного закладу:

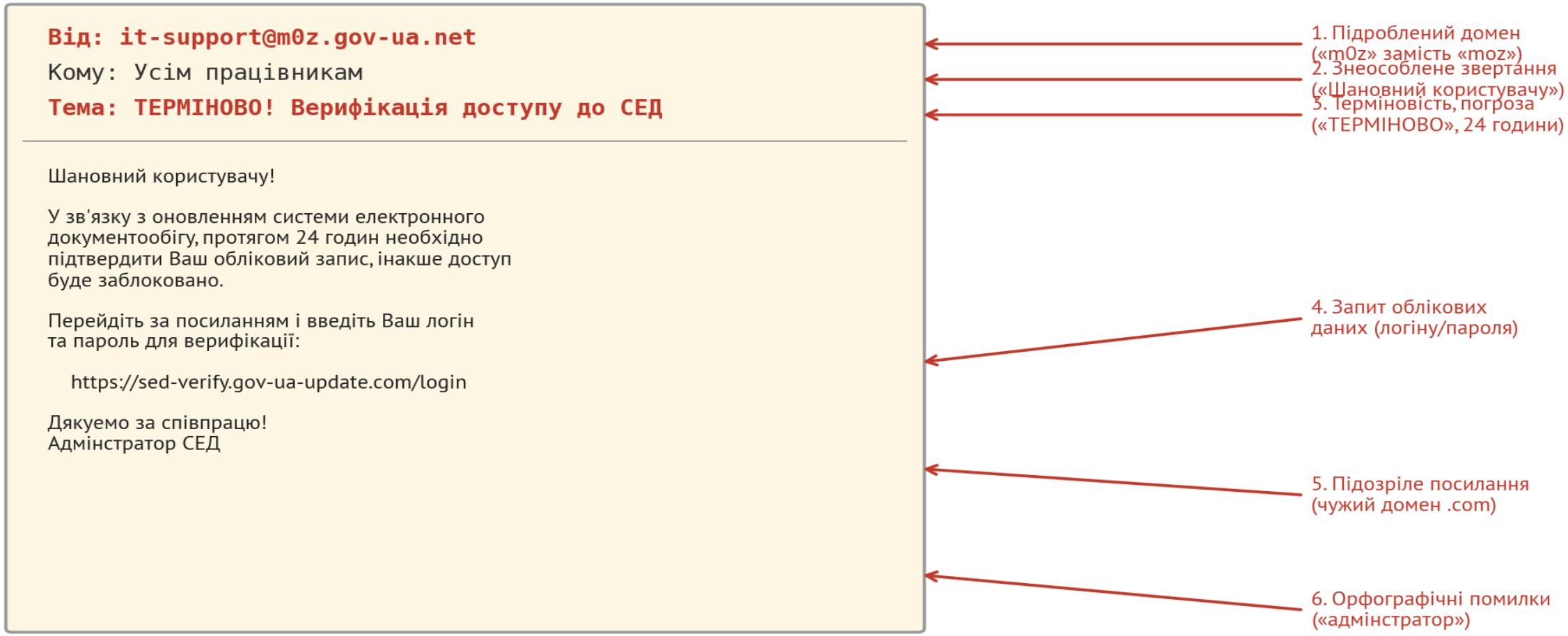
- **Вкладення в електронному листі (.docm, .xlsm, .zip, .iso)**
- **Перехід за посиланням і завантаження «оновлення» / «драйвера»**
- **Заражений USB-носій, підключений до робочого ПК**
- **Експлуатація неоновленого програмного забезпечення**

Наслідки для лікарні: зупинка прийому, втрата історій хвороб, штрафи за порушення обробки персональних даних.

РОЗДІЛ 3. ЯК РОЗПІЗНАТИ ФІШИНГОВИЙ ЛИСТ

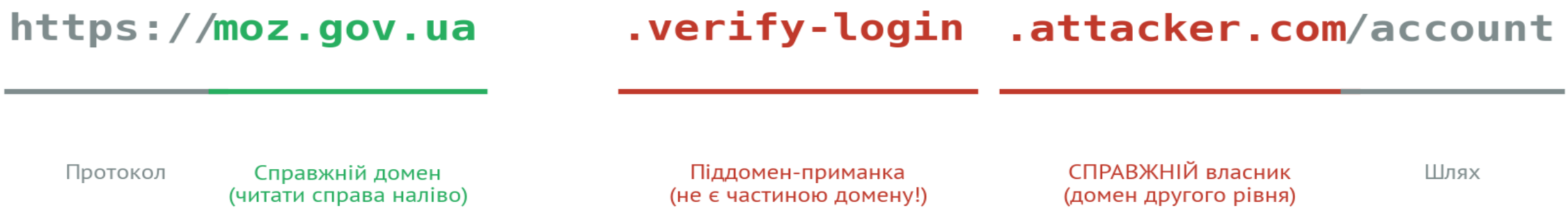
Анатомія фішингового листа: 6 ознак

Анатомія фішингового листа: 6 ознак, на які варто звернути увагу



Як читати посилання: справжній домен — праворуч

Як читати URL-адресу: де знаходиться справжній домен



ПРАВИЛО: справжній домен — це останні два сегменти ПЕРЕД першою «/».
У прикладі вище справжній домен — attacker.com, а не moz.gov.ua.

Правило читання URL — основа гігієни перевірки посилань.

Чек-лист: 10 секунд перед кліком

1. Чи я очікую цей лист? (від цього відправника, на цю тему)

2. Чи правильно написаний домен відправника? (m0z ≠ moz)

3. Чи звертаються до мене на ім'я, чи знеособлено?

4. Чи створюється штучна терміновість, страх, погроза?

5. Чи просять ввести пароль / код / банківські реквізити?

6. Чи збігається текст посилання з реальним URL (наведіть курсор!)?

7. Чи є вкладення з підозрілим розширенням (.exe, .zip, .iso, .docm)?

8. Чи є очевидні орфографічні помилки?

≥ 2 «так» на пункти 2–8 → не клікати, переслати в IT-відділ

РОЗДІЛ 4. БЕЗПЕЧНА РОБОТА З ПОШТОЮ ТА ІНТЕРНЕТ

Чого НЕ можна робити

✗ Відкривати вкладення від невідомих адресатів

✗ Переходити за посиланнями з незапитуваних листів

✗ Повідомляти паролі чи PIN-коди КЕП — навіть «ІТ-працівнику» по телефону

✗ Встановлювати самовільно програми, розширення браузера, VPN, анонімайзери

✗ Передавати службову інформацію через відкриті файлообмінники

✗ Завантажувати / запускати файли з розширеннями

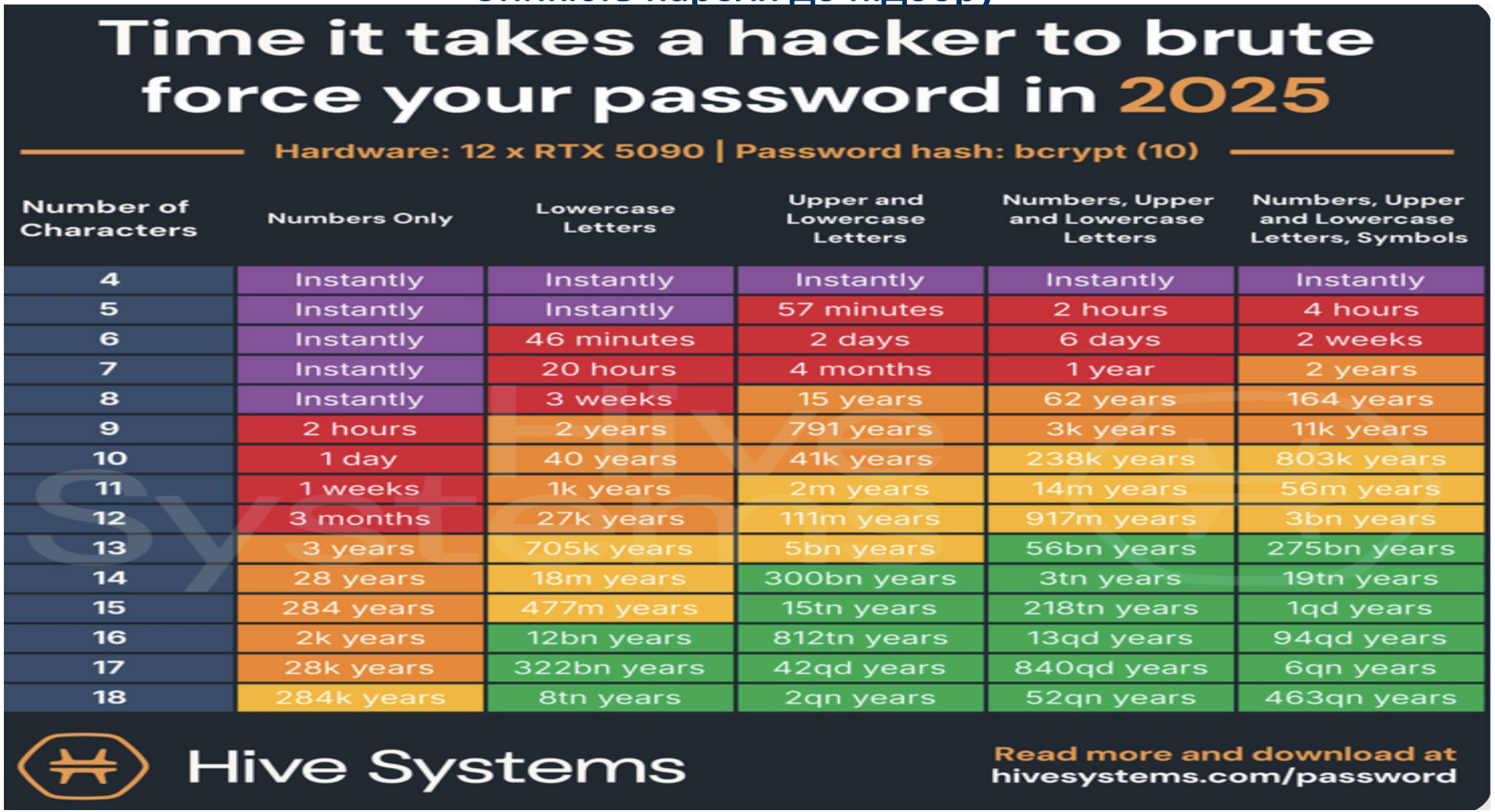
.exe, .bat, .cmd, .reg, .com, .vbs, .msi, генератори ключів

✗ Поширювати матеріали, заборонені законодавством України

✗ Поширювати матеріали, захищені авторськими правами

РОЗДІЛ 5. ПАРОЛІ ТА ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ

Стійкість пароля до підбору



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Як створити надійний пароль

Інструкції для створення:

- **Мінімум 8 символів (краще — 12+)**
- **Великі та малі літери, цифри, спецсимволи (! @ # $ % ^ & *)**
- **НЕ базується на персональних даних (прізвище, дата народження)**

Метод ідентифікаційної фрази:

1. Придумайте фразу: «Моєму сину Павлу три роки»

2. Перші літери: м с П т р

3. Ускладніть: M$п3P0ky! → такий пароль легко згадати, важко підібрати

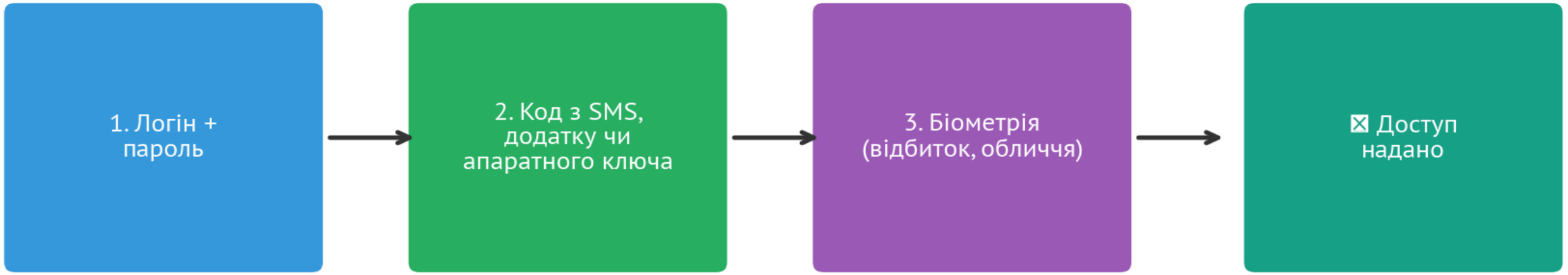
(час підбору такого паролю згідно таблиці – 11 тисяч років)

КРИТИЧНО важливе правило: один пароль — один сервіс

Окремий пароль для робочих та особистих ресурсів — ОБОВ'ЯЗКОВО

Двофакторна автентифікація (2FA / MFA)

Двофакторна автентифікація (2FA / MFA): як це працює



Навіть якщо зловмисник дізнається ваш пароль, без другого фактора він не отримає доступ.

РОЗДІЛ 6. РОБОЧЕ МІСЦЕ, ЗМІННІ НОСІЇ ТА ШІ

Правило «чистого екрана» і знайдені носії

Чистий екран (Інструкції):

- **Залишаєте робоче місце — БЛОКУЙТЕ екран: Win + L (Windows)**
- **Документи з обмеженим доступом — не залишати у видимості сторонніх**

USB-атака («підкинута флешка»):

- **Знайдена флешка на парковці / у коридорі / на ресепшні —**

  це ймовірно ПРИМАНКА (BadUSB, шкідливе ПЗ, що запускається при підключенні)
- **Категорично НЕ підключати до робочого ПК**
- **Передати ІТ-відділу для безпечного аналізу**
- **Флешки від співробітників, студентів та аспірантів перед використанням обов’язково перевіряти на наявність шкідливого ПЗ, використовуючи антивірус**

Безпечне використання ШІ

Категорично НЕ передавайте у ChatGPT, Gemini, Copilot та подібні системи:

- **Персональні дані пацієнтів (ПІБ, діагнози, ідентифікаційні дані)**
- **Службову інформацію з обмеженим доступом**
- **Внутрішні документи установи, протоколи, скани з печатками**
- **Облікові дані, токени, ключі API, фрагменти конфіденційного коду**

Що ВАЖЛИВО розуміти:

- **Дані, надіслані в публічну LLM, можуть зберігатися, використовуватися для навчання моделей і потенційно «вспливати» у відповідях іншим**
- **Для роботи з чутливими даними — лише санкціоновані установою рішення (локальні моделі, корпоративні Enterprise-версії з контролем даних)**

Чого НЕ змінювати самостійно

Без узгодження з ІТ-відділом установи КАТЕГОРИЧНО не дозволено:

✗ Зупиняти або вимикати антивірус та інші засоби захисту

✗ Змінювати налаштування поштового та веб-клієнта (правила пересилки!)

✗ Встановлювати програми з невідомих джерел

✗ Додавати свій обліковий запис до груп з підвищеними привілеями

✗ Підключати робочий ПК до неперевірених Wi-Fi мереж

Окрема загроза: правила автоматичної пересилки

(зловмисник, отримавши доступ, налаштовує тиху пересилку всієї пошти собі)

РОЗДІЛ 7. ДІЇ У РАЗІ ВИЯВЛЕННЯ КІБЕРЗАГРОЗИ

Індикатори компрометації — на що звернути увагу

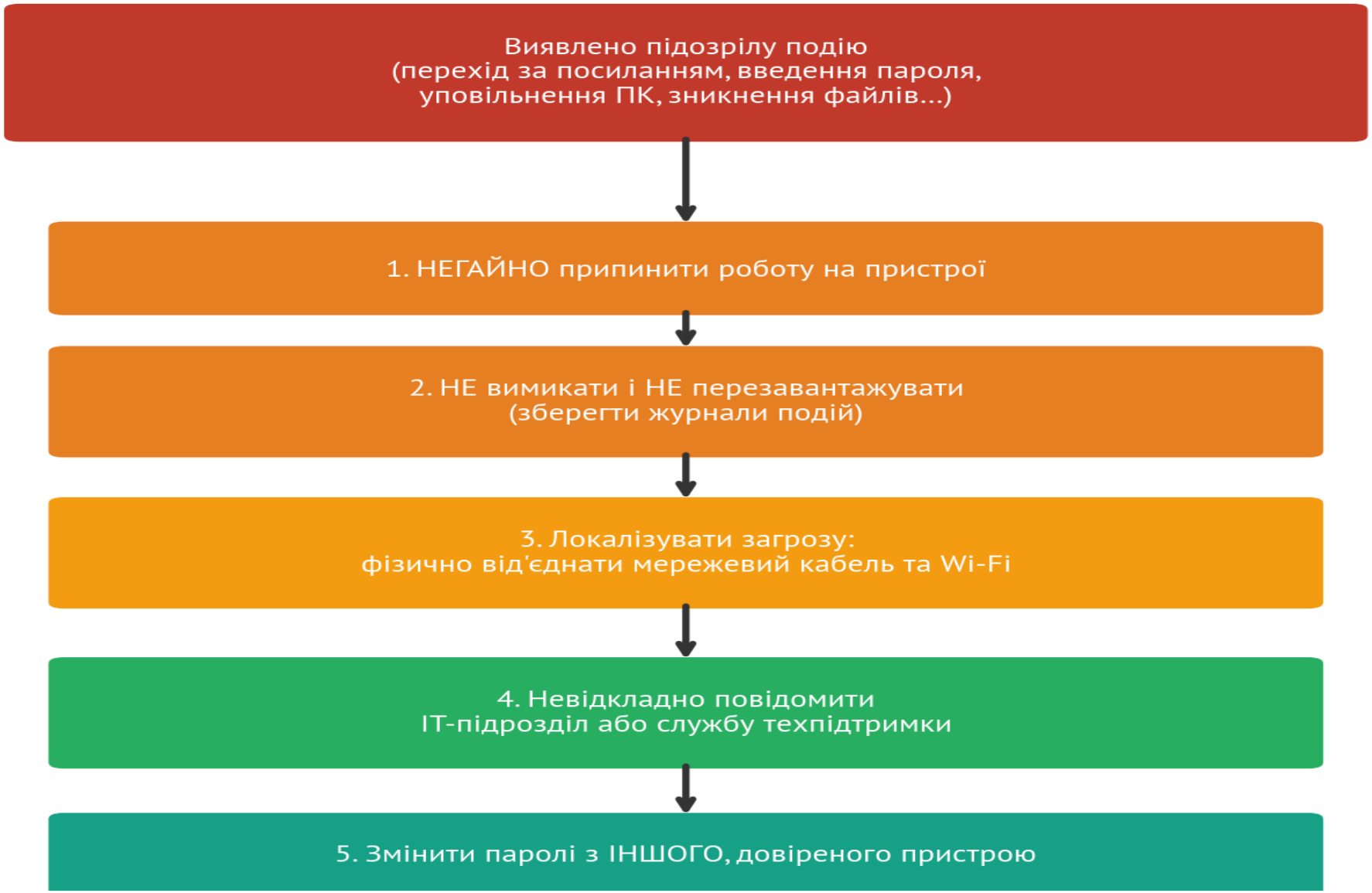
Технічні:

- **Раптове значне уповільнення роботи комп'ютера**
- **Зникнення, перейменування або спотворення файлів**
- **Незрозумілі повідомлення про помилки, спливаючі вікна**
- **Нетипова активність мережевого індикатора у бездіяльному режимі**
- **Вимога ввести пароль у місцях, де його раніше не запитували**

Поведінкові:

- **Колеги отримують від вас листи, яких ви не надсилали**
- **У «Надіслані» з'являються листи, яких ви не писали**
- **Невідомі правила в налаштуваннях пошти**
- **Несподівані входи у вашу пошту з інших країн (історія входів)**

Алгоритм дій при підозрі на кіберінцидент



Куди повідомляти про кіберінцидент

Перший контакт — IT-підрозділ вашої установи (телефонувати, не писати!)

Обмін інформацією про загрози — мережа MISP:

https://cert.gov.ua/article/39962

Корисні ресурси для самонавчання:

- https://moz.gov.ua/uk/kiberbezpeka
- https://www.youtube.com/watch?v=54y73kHuI6M
- https://www.hivesystems.com/password-table
- https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector
- https://www.enisa.europa.eu/publications/health-threat-landscape
- https://www.nist.gov/cyberframework

РОЗДІЛ 8. ПІДСУМКИ

10 золотих правил кібергігієни наукового та медичного працівника

1. Не очікую листа — отже, перевіряю відправника і не клікаю наосліп

2. Жоден реальний IT-фахівець ніколи не просить мій пароль

3. Терміновість і страх (залякування) у листі — ознака маніпуляції, а не вимоги

4. Перед кліком — навожу курсор, читаю URL справа наліво

5. Унікальний пароль 12+ символів для кожного важливого сервісу

6. 2FA увімкнено на пошті, банкінгу, Дії та робочих системах

7. Відходжу від ПК — Win+L. Знайшов флешку — несу в IT-відділ

8. У ChatGPT/Gemini/Copilot не вводжу дані пацієнтів та службову інформацію

9. У разі підозри: припинити роботу → не вимикати → від'єднати кабель Інтернету → дзвонити в IT

10. Сумніваєшся — спитай. Краще 1 хвилина перевірки, ніж тиждень відновлення