КОНТРОЛЬНИЙ СПИСОК

Перевірте паролі, сторонні входи та робочі комп'ютери

Злочинці продають викрадені паролі для доступу до робочих систем.

ЩО ВСЕРЕДИНІ

- [ ] **Як виявити викрадені паролі**
- [ ] **Як перевірити й закрити сторонні входи**
- [ ] **Що робити із зараженим комп'ютером**

Для: Власники компаній, керівники, бухгалтери та IT-відповідальні · ~15 хв

🖨️ **Остання сторінка для друку**

Veiltrack

Незалежне тестування безпеки

Ситуація

Поліція дев'яти країн разом із Європолом зупинила сервери трьох шкідливих програм і отримала понад шість мільйонів викрадених даних для входу. Їх продавали іншим злочинцям.

Працівник міг відкрити підроблений документ, а шкідлива програма викрасти паролі до робочої пошти.

Зміна пароля не завжди закриває сторонній доступ. Перевірте акаунти, активні входи та пристрої.

КОНТРОЛЬНИЙ СПИСОК

01 / 06

Перевірте повідомлення про витоки

ЯК МАЄ БУТИ

Відповідальний перевіряє робочі адреси, сповіщення та записує результати.

ЯК ПЕРЕВІРИТИ

Перевірте адреси через Have I Been Pwned. Перегляньте сповіщення й запишіть підозрілі акаунти.

> ОЗНАКА ПРОБЛЕМИ
>
> Є повідомлення про викрадений пароль, але акаунт не перевірили.

ЩО ЗРОБИТИ

Призначте відповідального, налаштуйте сповіщення та перевірте згадані акаунти.

КОНТРОЛЬНИЙ СПИСОК

02 / 06

Перевірте незнайомі входи

ЯК МАЄ БУТИ

Адміністратор звірив незнайомі входи з працівниками та записав підтверджені.

ЯК ПЕРЕВІРИТИ

Перегляньте історію входів у пошті й важливих системах. Уточніть у працівників незнайомі пристрої та час.

ОЗНАКА ПРОБЛЕМИ

Працівник не впізнає успішний вхід до акаунта.

ЩО ЗРОБИТИ

Збережіть записи підозрілих входів. Доручіть перевірити й обмежити сторонній доступ.

03 / 06 ВИСОКИЙ РИЗИК

Ізолюйте підозрілі комп'ютери

З'ясуйте, де використовували викрадений пароль. Перегляньте попередження захисту й результати перевірки на шкідливі програми.

> Захист виявив шкідливу програму, але робота триває.

→ Відключіть пристрій від мережі й передайте фахівцю.

04 / 06 ВИСОКИЙ РИЗИК

Закрийте сторонні входи

Перегляньте активні входи та пристрої. Звірте незнайомі з працівниками й перевірте можливість завершення.

> Сторонній пристрій досі має доступ до акаунта.

→ Завершіть сторонні входи. Повторно перевірте історію та доступ.

КОНТРОЛЬНИЙ СПИСОК

ВИСОКИЙ РИЗИК

05 / 06

Замініть викрадені паролі

ЯК МАЄ БУТИ

Працівник замінив пароль усюди, де повторював його. Відповідальний перевірив.

ЯК ПЕРЕВІРИТИ

З'ясуйте, де повторювали пароль. Перевірте його заміну та способи відновлення доступу.

ТРИВОЖНИЙ ЗНАК

Викрадений пароль досі працює в робочому акаунті.

ЩО ЗРОБИТИ

Замініть повторювані паролі з перевіреного пристрою. Видаліть незнайомі способи відновлення.

КОНТРОЛЬНИЙ СПИСОК

06 / 06

Увімкніть додаткове підтвердження входу

ЯК МАЄ БУТИ

Для входу до пошти й важливих систем працівникам потрібне додаткове підтвердження.

ЯК ПЕРЕВІРИТИ

Перевірте налаштування пошти й важливих систем. Переконайтеся, що кожен користувач підтверджує вхід додатково.

> ОЗНАКА ПРОБЛЕМИ
>
> До робочої пошти можна увійти лише за паролем.

ЩО ЗРОБИТИ

Увімкніть додаткове підтвердження й перевірте його з користувачами.

КОНТРОЛЬНИЙ СПИСОК

ГОТОВА ФРАЗА

Як перевірити незнайомий вхід у працівника

«Бачимо вхід до вашого акаунта з незнайомого пристрою. Це ви? Якщо ні, повідомте відповідальному. Не надсилайте пароль чи код підтвердження.»

ЧОГО НЕ РОБИТИ

Звертайтеся перевіреним каналом, не через підозрілий акаунт.

КОНТРОЛЬНИЙ СПИСОК

● ДІЙТЕ ОДРАЗУ

Що робити після крадіжки пароля або стороннього входу

1. Обмежте доступ. Збережіть історію входів і час подій.
2. Відключіть пристрій від мережі. Не вводьте нові паролі.
   За ознак зараження.
3. Завершіть сторонні входи. Змініть пароль із перевіреного пристрою. Перевірте відновлення доступу.
4. Перевірте пересилання пошти й доступ до даних. Запишіть результати.
   Якщо злам підтверджено або наслідки невідомі.

Незнайомий вхід не завжди означає злам чи витік даних.

VEILTRACK

Незалежне тестування безпеки

ДЛЯ ДРУКУ · ПАМ’ЯТКА КОМАНДІ

Як захистити робочі акаунти після крадіжки паролів

Роздрукуйте й роздайте відділу. 30 днів тримайте перед очима й позначайте день, коли діяли за пам’яткою. Коли це стане звичкою, аркуш можна зняти.

Щодня переглядайте сповіщення. Незнайомі входи звіряйте з працівниками:

- [ ] Перевіряю сповіщення й записую підозрілі акаунти.
- [ ] Звіряю незнайомі входи з працівниками.
- [ ] Не користуюся зараженим пристроєм до перевірки.
- [ ] Закриваю сторонні входи й перевіряю повторні.
- [ ] Замінюю паролі й перевіряю відновлення доступу.
- [ ] Перевіряю додаткове підтвердження для працівників.

30 ДНІВ ДО ЗВИЧКИ: ПОЗНАЧТЕ ДЕНЬ

	Пн	Вт	Ср	Чт	Пт
ТИЖДЕНЬ 1	☐	☐	☐	☐	☐
ТИЖДЕНЬ 2	☐	☐	☐	☐	☐
ТИЖДЕНЬ 3	☐	☐	☐	☐	☐
ТИЖДЕНЬ 4	☐	☐	☐	☐	☐

Ім’я, відділ: _____ Старт: _____

Питання щодо безпеки? Напишіть нам



Vlad Kraevsky
засновник Veiltrack

WEB
veiltrack.io

EMAIL
vlad@veiltrack.io