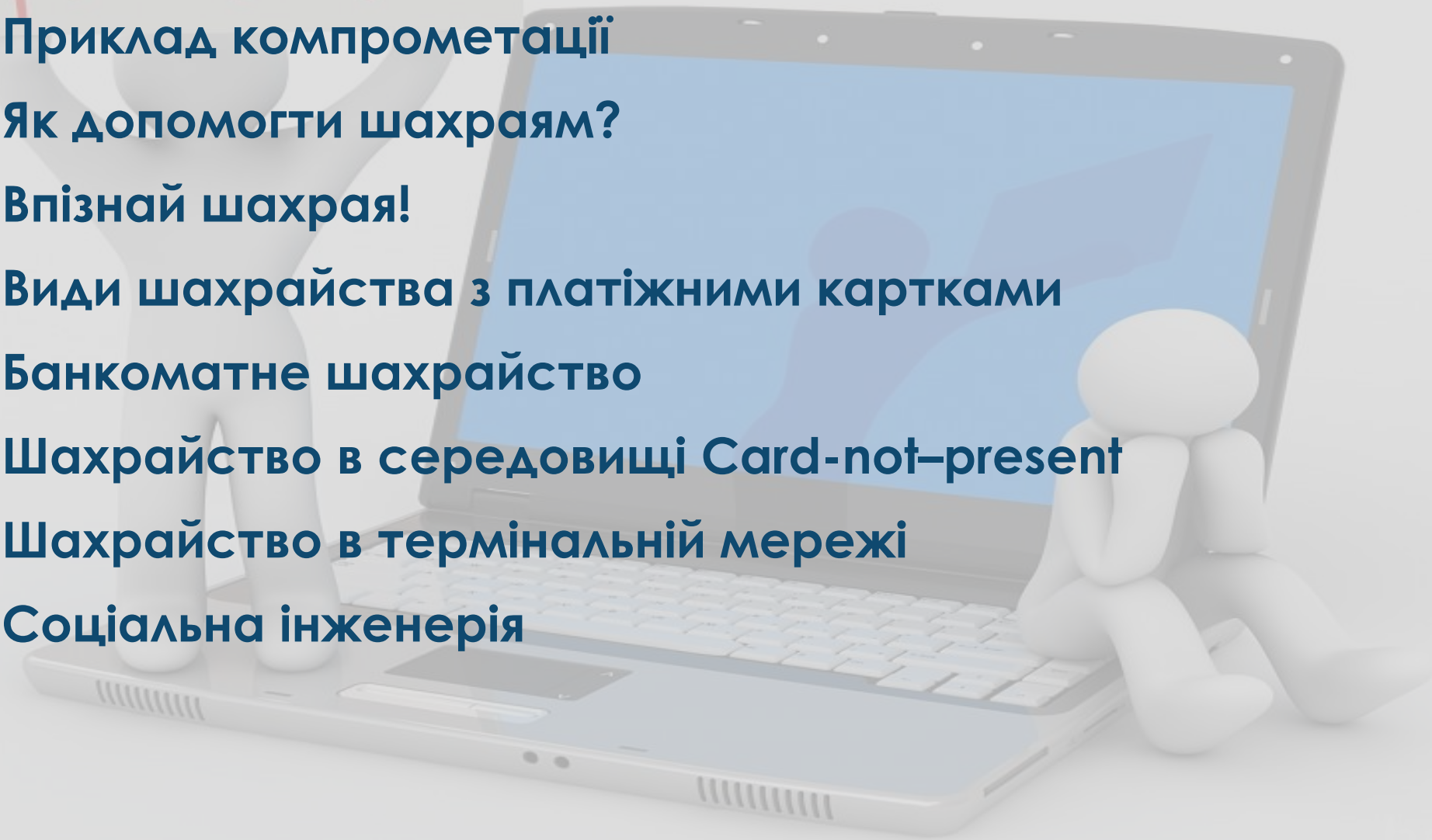
BANK ALLIANCE
АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК АЛЬЯНС»

Шахрайство з платіжними картками

BANK ALLIANCE
АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК АЛЬЯНС»

ЗМІСТ



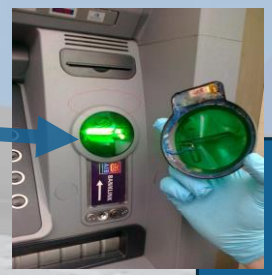
- ✓ Приклад компрометації
- ✓ Як допомогти шахраям?
- ✓ Впізнай шахрая!
- ✓ Види шахрайства з платіжними картками
- ✓ Банкоматне шахрайство
- ✓ Шахрайство в середовищі Card-not–present
- ✓ Шахрайство в термінальній мережі
- ✓ Соціальна інженерія

ПРИКЛАД КОМПРОМЕТАЦІЇ

Фізичний скімінг (Skimming)

За допомогою спеціальних пристроїв злочинці копіюють дані і в подальшому виготовляють дублікати карток, так званий «білий пластик», за яким отримують гроші

Встановлення міні-камери, таким чином шахраї дізнаються ПІН-код



На картоприймач встановлюють скімінговий пристрій.
Він зчитує і копіює дані банківської карти

ЯК ДОПОМОГТИ ШАХРАЯМ?

- Надавати номер карти / строк дії / CVV
- Надавати/повідомляти СМС-інформування від Банку
- Повідомляти особисті дані / ПІН-коди / паролі

Компрометація — ситуація, при якій реквізити банківської картки стали відомі іншій особі, в результаті чого її подальше використання є небезпечним і може призвести до несанкціонованого списання коштів з рахунку

ВПІЗНАЙ ШАХРАЯ!

Ким представляються шахраї:

- співробітником Банку
- співробітником поліції
- співробітником Пенсіонного фонду
- покупцем Вашого товару в Інтернеті

Що робити:

- У разі підозри, телефонуйте на офіційні номери Банку
- Не повідомляйте жодної інформації про свою карту
- Не повідомляйте секретні коди, дівоче прізвище матері, паролі з СМС-повідомлень
- Не розголошуйте особисті дані
- Не передзвонюйте на номери шахраїв, телефонуйте на офіційні номери Банку (є на сайті, в договорі, на платіжній картці)
- Підключить СМС-повідомлення для відстеження руху коштів

Що говорять шахраї:

- На вашу карту здійснюють напад
- Банк покращує заходи безпеки
- Якщо телефонують з «СБУ» — вимагають дані без пояснень
- Карту заблоковано з технічних причин

ВИДИ ШАХАРАЙСТВА З ПЛАТІЖНИМИ КАРТКАМИ

Банкоматне шахрайство

- Фізичний скімінг (Skimming)
- Cash Trapping
- Transaction Reversal Fraud (TRF)
- Програмний скімінг (Cyber Skimming)
- Прямий диспенс (Jackpotting)

Шахрайство в середовищі **Card-Not-Present**

- Фішинг
- Віруси на комп'ютерах і мобільних пристроях

Шахрайство в термінальній мережі

- Фізичний скімінг (Skimming)
- Програмний скімінг (Cyber Skimming)

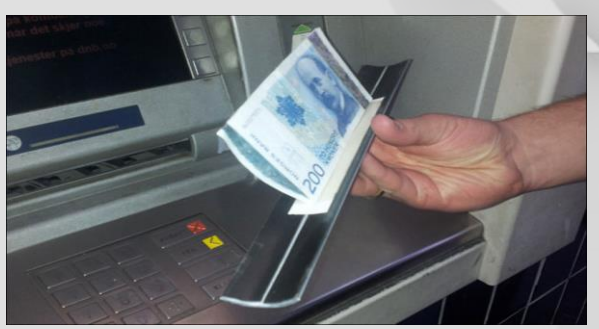
Соціальна інженерія

Вішинг

БАНКОМАТНЕ ШАХРАЙСТВО

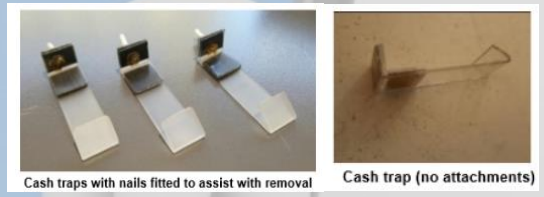
- **Фізичний скімінг (Skimming)**

Полягає у встановленні зловмисниками на банкоматі обладнання для копіювання даних магнітної смуги та запису ПІН-коду платіжної картки



- **Cash Trapping**

Полягає у встановленні зловмисником на банкоматах спеціальних пристроїв, які дозволяють здійснити захват готівки за операціями, які здійснюють законні держателі карток. В результаті держатель картки відходить від банкомату, не отримавши готівку, а зловмисник підходить до банкомату і привласнює захвачені шахрайським пристроєм банкноти



- **Transaction Reversal Fraud (TRF)**

<u>Здійснюється в 2 етапи:</u>

1. Зловмисник проводить в банкоматі операцію видачі готівки на мінімально можливу суму, під час якої у відкритий шатер розміщується спеціальний пристрій типу «виделка»

2. Зловмисник проводить в банкоматі операцію видачі готівки на максимально можливу суму, під час якої банкноти залишаються у виделці, а банкомат автоматично генерує операцію типу Reversal на картковий рахунок

В результаті зловмисник отримує готівку при фактично незмінному балансі карткового рахунку, за якими проводилась операція

- **Програмний скімінг (Cyber Skimming)**

Полягає у встановленні зловмисником на банкоматі шкідливого програмного забезпечення, яке здійснює копіювання даних магнітної смуги та ПІН-кодів платіжних карток

- **Прямий диспенс (Jackpotting)**

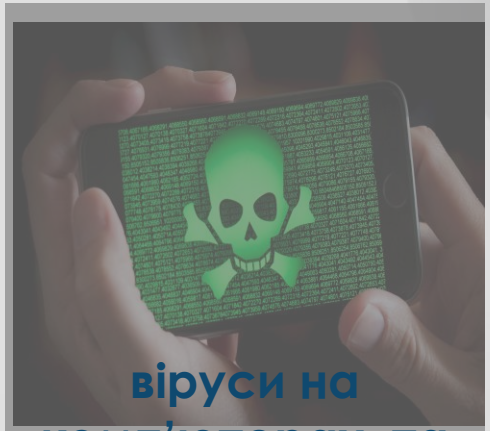
Полягає у встановленні та активації зловмисником на банкоматі шкідливого програмного забезпечення (ПЗ), яке дає диспенсеру банкомата команду на видачу всіх банкнот завантажених в касети

Виділяють два основні типи актуальних атак:

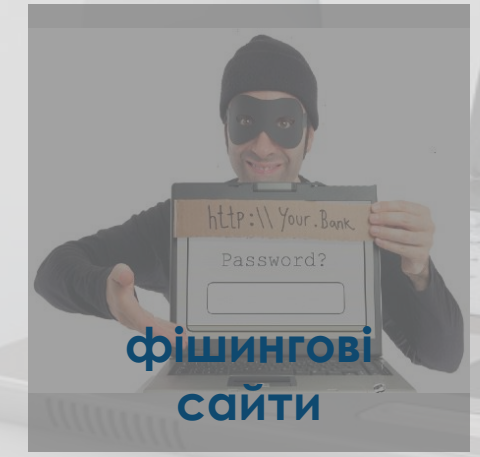
- - з використанням шкідливого ПЗ Backdoor.PadPin
- - з використанням пристроїв типу BlackBox

ШАХРАЙСТВО В СЕРЕДОВИЩІ CARD-NOT-PRESENT

Основними джерелами компрометації даних залишаються:

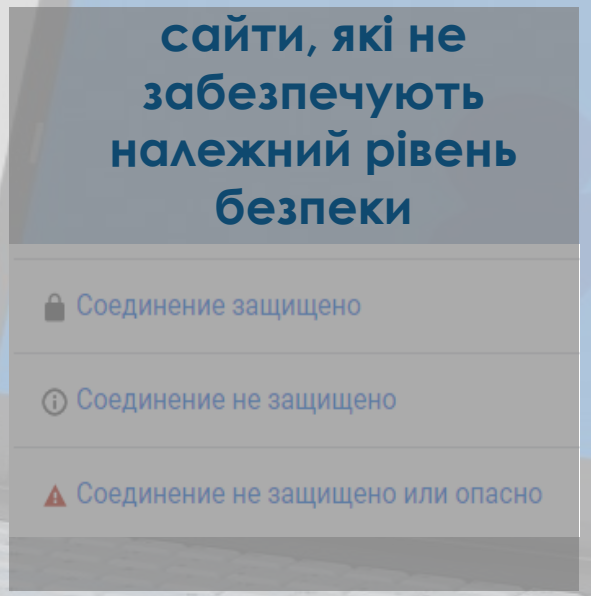


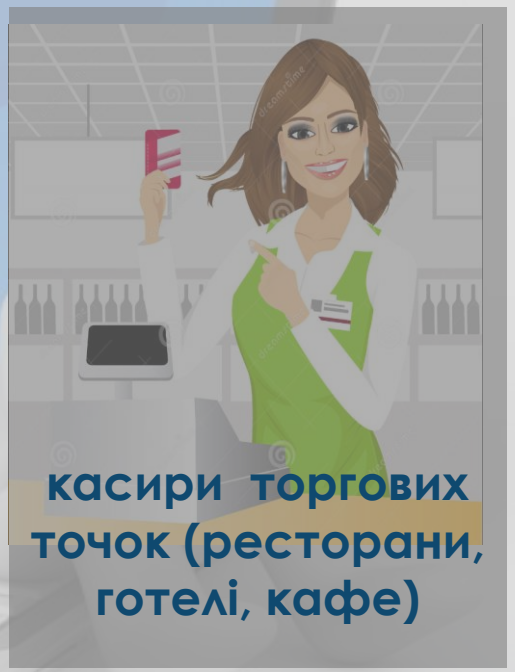
віруси на комп'ютерах та мобільних пристроях



фішингові сайти

сайти, які не забезпечують належний рівень безпеки





касири торгових точок (ресторани, готелі, кафе)

ШАХРАЙСТВО В ТЕРМІНАЛЬНІЙ МЕРЕЖІ

Основні схеми шахрайства

Встановлення фізичного скімінгу, компрометація на рівні торговця

Фіктивні торговці

Мета — використання підроблених карток/реквізитів карток

Компрометація на рівні баз даних іноземних еквайрів/великих еквайрінгових мереж

Ведення торговцем подвійної діяльності в Інтернеті — легітимною в зоні доменів .UA *(наприклад, туристичні послуги)* та забороненої поза доменами .UA *(наприклад, продаж медичних препаратів або тютюнових виробів в США)*

Основні канали контакту зловмисників:

- Інтернет-аукціони та дошки оголошень
- соціальні мережі
- електронна пошта
- мобільний телефон
- анкети різноманітних бонусних програм

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Сутність шахрайства полягає у мотивації шахраєм клієнта банку до здійснення дій, які він за інших обставин в звичайній обстановці, маючи час на обміркування та можливість порадитись з іншими людьми, не здійснив би

Зловмисники стимулюють клієнтів

здійснювати перекази своїх коштів на карткові рахунки шахраїв *(банкомати або системи Інтернет-банкінгу)*

розголошувати реквізити своїх платіжних карток та/або свої персональні дані, необхідні для проведення операцій в мережі Інтернет

надавати копії документів, що ідентифікують особу, та можуть бути використанні при оформленні споживчих та грошових кредитів

BANK ALLIANCE
АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК АЛЬЯНС»

Дякуємо за увагу!