# ШАХРАЙСЬКІ АТАКИ, МІШЕНЬЮ ЯКИХ Є ПЕРСОНАЛ КОМПАНІЇ
# ЯК СЕБЕ ЗАХИСТИТИ

**МІШЕНЬ**
Менеджери та фахівці середньої ланки в сфері надання фінансових послуг та матеріально-технічного забезпечення

**ВИСОКА ПРИВАБЛИВІСТЬ ЗЛОЧИНУ**
Великі прибутки та невеликий ризик бути викритим

Суттєві фінансові наслідки для компаній, що стали об'єктом атаки
**ВТРАТИ У РОЗМІРІ МІЛЬЙОНІВ ЄВРО**

**КАДРОВІ ВТРАТИ**
Ганьба, покарання, втрата роботи

# ДІЗНАЙТЕСЬ ПРО АКТУАЛЬНІ СХЕМИ ШАХРАЙСТВА

EUROPOL
ЄМА

## ПІД ВИГЛЯДОМ КЕРІВНИКА

### КРОК 1
Шахрай телефонує співробітнику, видаючи себе за керівника вищої ланки (напр., керівника або фінансового директора компанії)

### КРОК 2
Вимагає здійснити негайний грошовий переказ, наголошуючи на необхідності збереження конфіденційності

### КРОК 3
Посилається на скрутні обставини, в яких перебуває компанія (напр., податкова перевірка, злиття або поглинання компанії)

### КРОК 4
Змушує співробітника не дотримуватися встановленої процедури авторизації

### КРОК 5
Пояснює, як діяти за вказівками, що будуть надалі надходити від сторонньої особи або електронною поштою

### КРОК 6
Співробітник переказує кошти на рахунок, який знаходиться під контролем шахрая. Після того гроші переказуються на інші рахунки, що відкриті закордоном

**ВАРІАЦІЇ**
- Вимагає надати інформацію про клієнтів компанії (напр., відомості про всі несплачені рахунки)
- Використовує отриману інформацію для привласнення коштів клієнтів компанії

## ПІД ВИГЛЯДОМ ЗЛАМУ СИСТЕМИ

### КРОК 1
Шахрай телефонує співробітнику, видаючи себе за IT-спеціаліста компанії (або банківського працівника)

### КРОК 2
Повідомляє про здійснення зламу системи компанії (або системи Інтернет-банкінгу)

### КРОК 3
ВАРІАНТ 1: Вимагає надати фінансову інформацію під приводом перевірки та/або налаштування програми віддаленого адміністрування

ВАРІАНТ 2: Змушує співробітника зателефонувати до банку. Використовує технологію, що дає змогу залишатися на лінії зв'язку після закінчення телефонної розмови, та підслуховує конфіденційну інформацію, що надається співробітником компанії працівнику банку (номери рахунків, паролі)

### КРОК 4
Отримана інформація /доступ використовуються для переказу коштів з рахунку компанії на рахунок шахрая

**ВАРІАЦІЇ**
- Змушує переказати кошти на інший «безпечний» рахунок
- Співробітник переказує кошти на рахунок, який знаходиться під контролем шахрая. Після того гроші переказуються на інші рахунки, що відкриті закордоном

## ПІД ВИГЛЯДОМ ПОСТАЧАЛЬНИКА

### КРОК 1
Шахрай звертається до співробітника телефоном або електронною поштою, видаючи себе за одного з постачальників компанії (напр., постачальника сировини або послуг)

### КРОК 2
Повідомляє про зміну реквізитів рахунку для перерахування коштів постачальнику за послуги / матеріали

### КРОК 3
Вимагає здійснити наступний платіж за новими реквізитами

### КРОК 4
Співробітник викриває шахрайство, коли отримує скарги від справжнього постачальника про несплачені рахунки

**ВАРІАЦІЇ**
- Шахрай звертається до постачальника під виглядом представника іноземної підрядної компанії
- Видає себе за стратегічного партнера або відому комерційну компанію
- Замовляє купівлю великого обсягу товарів з відстроченням сплати
- Постачальник товари відвантажує, але гроші за них не отримує

## ЯК ШАХРАЇ ПРИХОВУЮТЬ ІНФОРМАЦІЮ ПРО СЕБЕ ТА СВОЄ МІСЦЕЗНАХОДЖЕННЯ?

- Використовують підроблені документи, які містять логотип / підписи керівників компанії, зображення яких було знайдено в Інтернет
- Підробляють адреси електронної пошти відправників
- Підміняють номери, з яких телефонують, на номери тих, за кого себе видають
- Використовують VOIP та проксі-сервери
- Використовують послуги підпільних колл-центрів

## ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

**ЗАГРОЗА:**

Проникає до корпоративної мережі

Отримує доступ до інформації, що підриває репутацію компанії, про:
- протизаконні банківські перекази
- використання банківського рахунку для фінансових махінацій
- промислове шпигунство

Отримує доступ до інформації партнерів/клієнтів для:
- перепродажу (злочин як Послуга);
- шахрайства з використанням платіжних карток

**ОТРИМУЄ ДОСТУП ЗА ДОПОМОГОЮ:**
- шкідливих програм, що розсилаються електронною поштою
- завантаження співробітником шкідливої програми
- зламу системи безпеки

# ЯК РОЗПІЗНАТИ

EUROPOL
ЄМА

- Несподіваний дзвінок / електронний лист, в якому запитують фінансову інформацію (номери рахунків, паролі)
- Несподіваний дзвінок / електронний лист, в якому запитують інформацію щодо внутрішніх процедур здійснення платежу або поставок
- Наполегливе вимагання виконати прохання/наказ
- Надзвичайна подія

### ПІД ВИГЛЯДОМ КЕРІВНИКА
- Особисте спілкування з керівником вищої ланки, з яким ви зазвичай не підтримуєте взаємні стосунки, діловий або дружній зв'язок
- Незвичайне розпорядження, що суперечить внутрішнім процедурам компанії
- Вимога щодо збереження конфіденційності
- Погрози або непритаманні лестощі / обіцянка відзнаки

### ПІД ВИГЛЯДОМ ЗЛАМУ СИСТЕМИ
- Тон мовлення IT-співробітника / співробітника служби безпеки, що має викликати тривогу, занепокоєння
- Вимога завантажити програмне забезпечення з підключенням до зовнішньої мережі (напр., під приводом перевірки та/або налаштування програми віддаленого адміністрування)
- Пропозиція переказати кошти на інший «безпечний» рахунок

### ПІД ВИГЛЯДОМ ПОСТАЧАЛЬНИКА
- Несподівана зміна контактної інформації / реквізитів рахунку іноземної підрядної компанії (як водиться, про зміну реквізитів рахунку повідомляється заздалегідь, за декілька тижнів / місяців)
- Зміна відбувається невдовзі після отримання великого замовлення або напередодні здійснення оплати

### ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
- Несподіваний електронний лист зі знеособленим привітанням
- Несподіваний електронний лист, що містить підозрілі гіперпосилання / URL-адреси

# ЯК ДІЯТИ

EUROPOL

- Будьте ОБІЗНАНИМИ із ризиками та розповсюдьте цю інформацію серед своїх колег.
- Будьте обачними, використовуючи соціальні мережі: поширюючи інформацію про своє місце роботи та посадові обов'язки, ви власноруч збільшуєте ризик стати мішенню для шахрайської атаки.
- Уникайте поширення чутливої інформації про структуру, безпеку та процедури компанії.
- Ніколи не переходьте за підозрілими гіперпосиланнями та не відкривайте сумнівних вкладень, отриманих електронною поштою. Будьте особливо пильними, коли переглядаєте листи з особистої поштової скриньки на службовому комп'ютері.
- Якщо ви отримали підозрілий електронний лист або дзвінок, обов'язково сповістить про це IT-службу вашої компанії: саме вони опікуються такими питаннями. IT-служба перевірить вміст підозрілого листа та у разі потреби заблокує одержання інших листів від його відправника.
- Завжди уважно перевіряйте адресу електронної пошти, якщо маєте справу з чутливою інформацією / грошовими переказами. Нерідко шахраї використовують підроблену адресу електронної пошти, яка може відрізнятися від справжньої лише однією літерою.
- Якщо ви отримали електронний лист або дзвінок, який сповіщає про злам системи, не надавайте інформацію / не здійснюйте грошовий переказ першої ж миті. Спершу потелефонуйте особі, від імені якої вам надійшов лист / дзвінок, використовуючи номер телефону з вашої телефонної книжки, телефонного довідника або офіційного сайту компанії, — не телефонуйте за номером, який було надано в електронному листі / під час телефонної розмови. Якщо вам телефонували, перетелефонуйте, використовуючи інший телефонний апарат (шахраї використовують технологію, що дає їм змогу залишатися на лінії зв'язку після закінчення телефонної розмови).
- У разі виникнення будь-яких сумнівів щодо платіжного доручення, завжди звертайтесь за порадою до колег, навіть якщо вас просили зберігати конфіденційність.
- Поміркуйте, з яким співробітником компанії в разі виникнення сумнівів радяться ваші колеги, — обговоріть це з ним також.
- Якщо постачальник повідомляє про зміну реквізитів рахунку, обов'язково зв'яжиться з ним, щоб підтвердити отриману інформацію. Зважайте на те, що в адресу електронної пошти / номер телефону, що зазначений на рахунку, могли бути внесені зміни.
- Дотримуйтесь політики безпеки компанії щодо здійснення платежів та поставок. Точно, без відхилень виконуйте всі вимоги, не оминаючи виконання жодної. Не піддавайтеся тиску.
- У разі спроби шахрайства завжди звертайтеся до Департаменту кіберполіції Національної поліції України, навіть якщо ви виявилися спроможними не пійматися в пастку шахраїв.