ЯК НЕ СТАТИ ЖЕРТВОЮ ШАХРАЙСТВА В ЕСТОНІЇ?

This material is part of the DEUCE project, implemented by the e-Governance Academy and funded by a grant from the United States Department of State. The opinions, findings, and conclusions stated herein are those of the author(s) and do not necessarily reflect those of the United States Department of State.

ОБЕРЕЖНО
ШАХРАЇ!!!

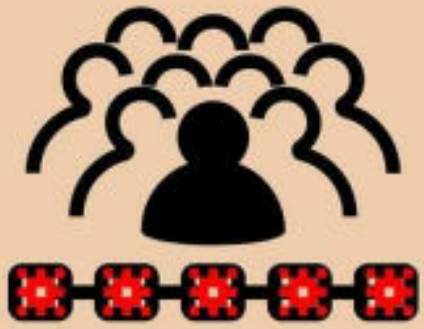
ВАШІ ГРОШІ – МОЯ МЕТА!

8,3 млн євро

втратили мешканці Естонії від шахрайських схем за 2023 рік.

7262 євро

середня шкода від шахраїв на одну жертву



1143 особи

мінімум стали жертвами шахрайства (за офіційними даними Департаменту поліції та прикордонної охорони Естонії)

Більшість постраждалих зіткнулася з різними інвестиційними та телефонними шахрайствами. Також розповсюджуються фішингові листи через мобільні телефони, інтернет-чати або електронну пошту.

Від телефонного шахрайства постраждали

524 ОСОБИ

Від інвестиційного шахрайства постраждали

305 ОСІБ

Через фішингові листи постраждали

314 ОСІБ

які в цілому втратили

3 МЛН ЄВРО

5 МЛН ЄВРО

300 ТИСЯЧ ЄВРО

Шахраї виступали від імені поліцейських, представників банків чи інших установ або "друзів" у соціальних мережах. Вони користуються спеціальними програмами, які генерують естонський номер, хоча дзвінок фактично робиться з-за кордону.

Не зважаючи на інформаційні компанії, які проводять різні організації, щодо небезпеки від шахрайства ми все одно "потрапляємо на гачок" таких чаклунів.

ЗВЕРНЕННЯ ВІД ШАХРАЇВ НАГАДУЄ ЗАКЛЯТТЯ

"Ви та ваші гроші в небезпеці!
І тільки ваші коди Smart ID, mobiil-ID та коди інтернет-банку здатні врятувати світ!".

Ми слухаємо та, наче під впливом магічних сил, збагачуємо шахраїв та допомагаємо їх імперії зростати.

ЯКІ ІНСТРУМЕНТИ ПСИХОЛОГІЧНОГО ТИСКУ ВИКОРИСТОВУЮТЬ ШАХРАЇ

і чому ми на них "ведемось"? (ч. 1)

Чому зловісні чари шахраїв мають над нами владу?

Тому що вони спираються на декілька простих, але дієвих інструментів психологічного тиску. Зловмисники добре знають, як використати наші емоції проти нас самих, навіть якщо ми багато чули про різні схеми шахрайства і почуваємось захищеними. Нижче ви знайдете основні інструменти, за допомогою яких шахраї беруть людей "на гачок":

Хибне почуття безпеки

Це перша пастка, у яку нас ловлять охочі до чужих грошей. Переконання, що "зі мною такого точно не може трапитись" знижує нашу пильність і робить нас більш вразливими.

> Зі мною такого точно не може трапитись!

> Зловмисники представляються робітниками банку або поліціянтами

Звернення до авторитетності

Шахраї діють за схожими схемами. Ключову роль в них часто відіграє важлива, значуща для нас людина або орган влади. Наприклад, зловмисники представляються поліціянтами, представниками державних органів або співробітниками банку. Злочинці можуть вдавати, ніби дзвонять від імені вашої дитини/батьків/бабусів та дідусів тощо.

Які інструменти психологічного тиску використовують шахраї (ч. 2)

Створення поспіху та напруги

Якщо ми зупинимось та подумаємо, чари шахраїв швидко розвіються. Саме тому вони так кваплять людей із прийняттям рішень, вдаючись до різних хитрощів. Наприклад, погрожуть тим, що ваші банківські рахунки буде от-от заблоковано, ваших близьких буде важче витягти з халепи або товар чи послуга, які нас приваблюють, закінчаться, якщо негайно не внести оплату.

Ефект потоку інформації

Також слугує для створення напруги. Людину буквально закидують надмірною кількістю подробиць, через що важко виділити більш вагому інформацію та зрозуміти, що вас обманюють.

Ефект якорування

Наш мозок схильний фокусуватись на першій отриманій інформації. Шахраї обертають це собі на користь, наприклад, пропонуючи спочатку високу ціну на товар, а потім знижуючи її. Через це наступні пропозиції здаються дуже привабливими і їх страшно упустити.

ЩО РОБИТИ

щоб не стати жертвою шахраїв

1 Перевіряйте джерела інформації

- Не відкривайте файли і не переходьте за посиланнями з листів від невідомих відправників.
- Завжди перевіряйте URL-адреси на правильність, щоб уникнути фішингових сайтів.

2 Використовуйте двофакторну аутентифікацію

Увімкніть двофакторну аутентифікацію для важливих облікових записів. Це додасть ще один рівень захисту, навіть якщо хтось дізнається ваш пароль.

3 Захищайте особисту інформацію

Ніколи не передавайте особисті дані, паролі, номери кредитних карток або іншу конфіденційну інформацію через електронну пошту або телефон.

4 Використовуйте складні паролі

Використовуйте складні та унікальні паролі для різних облікових записів. Використовуйте менеджери паролів для їх зберігання та генерації.

5 Оновлюйте програмне забезпечення

Встановлюйте всі оновлення програм та операційної системи. Оновлення часто містять виправлення безпеки, які захищають ваш пристрій від нових загроз.

6 Використовуйте антивірусні програми

Установлюйте надійне антивірусне та антишпигунське програмне забезпечення та регулярно скануйте систему

7 Будьте обережні з телефонними дзвінками

Якщо хтось телефонує та просить передати особисті дані чи паролі, завершіть дзвінок та передзвоніть до установи за офіційним номером.

8 Будьте скептичні до надмірних обіцянок

Якщо щось виглядає надто добре, щоб бути правдою (виграш в лотерею, в якій ви не брали участі чи спадок від невідомої троюрідної тітки), ймовірно, це шахрайство.

9 Перевіряйте фінансові операції

Слідкуйте за своїми фінансовими операціями та звітами. Якщо ви помітите підозрілі транзакції, негайно зв'яжіться зі своїм банком.

10 Навчайтеся розпізнавати шахрайство

Ознайомтеся з різними видами шахрайства, які використовують електронні засоби, та вчіть своїх близьких, як розпізнавати подібні атаки.

Протестувати рівень знань з кібербезпеки можна тут:

https://www.nvsorlik.ee/en/test

Дотримуючись цих простих правил, ви зможете значно знизити ризик стати жертвою шахраїв у цифровому світі.
Бережіть свої дані та будьте обережними!

ЩО РОБИТИ

якщо ви стали жертвою шахраїв

Якщо ви стали жертвою шахраїв через цифрові засоби, важливо швидко діяти, щоб мінімізувати шкоду і захистити свої дані.
Ось конкретні кроки, які слід зробити:

1 Зберігайте спокій і аналізуйте ситуацію

Заспокойтесь: Паніка може призвести до неправильних рішень. Спокійно оцініть ситуацію.

2 Змініть паролі

Негайно змініть паролі всіх облікових записів, які могли бути скомпрометовані. Використовуйте складні та унікальні паролі для кожного облікового запису.

3 Повідомте фінансові установи

- Негайно повідомте банк або кредитну компанію про шахрайство
- Перевірте останні транзакції на підозрілі операції; банки часто допомагають повернути гроші у разі доведеного шахрайства.

4 Повідомте відповідні служби

Заявіть про шахрайство до поліції, надавши всю доступну інформацію. Повідомте кіберполіцію (в Україні через їх сайт або за телефоном)

5 Використовуйте спеціалізовані служби

- Проведіть повне сканування пристрою антивірусними програмами для виявлення і видалення шкідливих програм.
- зверніться до фахівців з кібербезпеки для відновлення безпеки ваших даних і пристроїв.

Якщо було використано ваш телефонний номер, повідомте свого оператора, щоб заблокувати номер або змінити SIM-карту.
Повідомте свого інтернет-провайдера, якщо ви вважаєте, що ваш інтернет-зв'язок був скомпрометований.

6 Повідомте відповідні організації

7 Моніторинг та оновлення безпеки

Регулярно перевіряйте свої облікові записи на наявність підозрілої активності.
Увімкніть двофакторну аутентифікацію для всіх важливих облікових записів, якщо ви ще цього не зробили.

Повідомте своїх друзів, родичів та колег про інцидент, особливо якщо їх контакти могли бути скомпрометовані. Це допоможе їм бути обережними та уникнути можливих шахрайських схем.

8 Інформування про інцидент

9 Навчання на помилках

Проаналізуйте, як стався інцидент, що можна було зробити по-іншому і як уникнути подібних ситуацій у майбутньому.

Якщо ви втратили значну суму грошей або маєте інші серйозні наслідки, зверніться за юридичною допомогою для захисту своїх прав.

10 Отримання допомоги

Дотримуючись цих кроків, ви зможете мінімізувати наслідки шахрайства і захистити себе у майбутньому.

КУДИ ЗВЕРТАТИСЯ В ЕСТОНІЇ

Якщо ви стали жертвою телефонного шахрайства в Естонії, важливо діяти швидко і повідомити відповідні органи для отримання допомоги та захисту своїх прав:

1 ПОЛІЦІЯ 112

POLITSEI.EE

2 КІБЕРПОЛІЦІЯ

Якщо шахрайство стосується інтернету або кіберзлочинів, зверніться до відділу кіберполіції. Більше інформації можна знайти на Politsei.ee

3 ФІНАНСОВІ УСТАНОВИ

Негайно зв'яжіться зі своїм банком або кредитною організацією, щоб повідомити про шахрайство і заблокувати будь-які підозрілі транзакції.

PANGALIIT

Естонська банківська асоціація (Pangaliit) також може надати інформацію та допомогу. https://www.pangaliit.ee

4 СПОЖИВЧИЙ ЗАХИСТ

****620 1707****

Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA): Естонської агенції захисту прав споживачів та технічного нагляду можуть допомогти у випадках шахрайства.

5 КОНСУЛЬТАЦІЇ

NÕUSTAMISTELEFON

Естонія має консультаційні лінії для постраждалих від шахрайства, де можна отримати поради та інформацію.

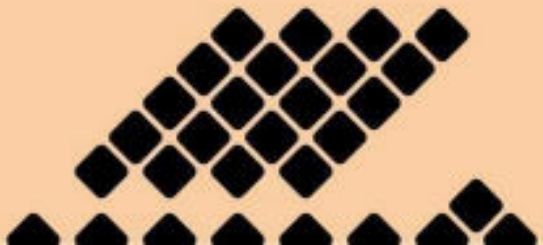
6 ОПЕРАТОР МОБІЛЬНОГО ЗВ'ЯЗКУ

ELISA, TELE2, TELIA

Зв'яжіться зі своїм оператором мобільного зв'язку, щоб заблокувати номер або змінити SIM-карту, якщо це необхідно.

7 ПОШИРЕННЯ ІНФОРМАЦІЇ

Повідомте про шахрайство в своїх соціальних мережах або зверніться до місцевих медіа



SCAM MAP PROJECT

Tallinn, 2024

This material is part of the DEUCE project, implemented by the e-Governance Academy and funded by a grant from the United States Department of State. The opinions, findings, and conclusions stated herein are those of the author(s) and do not necessarily reflect those of the United States Department of State.