Шахраї телефонують з телефонних номерів, які імітують офіційні номери телефонів банків або інших установ публічної довіри

- Повідомлення
FinCERT.pl – Банківського центру кібербезпеки Асоціації польських банків
Центрального бюро по боротьбі з кіберзлочинністю
Головного управління поліції
від 7 грудня 2022 року

Спуфінг (spoofing), тобто фальшиві телефонні дзвінки злочинців, які видають себе за працівників банків чи інших установ публічної довіри, таких як Асоціація польських банків, Управління комісії фінансового нагляду Польщі, ...!

Остерігайтеся телефонних дзвінків, під час яких шахраї представляються працівником банку або іншою особою, яка заслуговує на довіру (наприклад, працівником Управління комісії фінансового нагляду, працівником Групи безпеки банків в Асоціації польських банків або працівником поліції). Під час шахрайського дзвінка на Вашому телефоні може відображатися номер телефону або назва установи, якій Ви довіряєте.

Злочинець буде впливати на Ваші емоції, щоб викликати у Вас відчуття небезпеки, тривоги, занепокоєння або цікавості. Шахрай розмовлятиме з Вами українською, російською, рідше польською мовою.

Мета – отримати конфіденційну інформацію (логін і пароль до онлайн-банкінгу, BLIK-коди, дані платіжної картки) або переконати Вас виконати певні дії (наприклад, встановити програмний додаток, який дозволить зловмисникам отримати віддалений доступ до Вашого комп'ютера чи телефону).
Нижче наводимо приклади таких розмов:

Доброго дня, Ви підтверджуєте переказ на суму 800 злотих для пана Даріуша? ... Ні? Тоді нам потрібно швидко його заблокувати. Будь ласка, встановіть програму XXX, я допоможу Вам вирішити цю проблему.

Доброго дня, я працівник банку і звертаюся до Вас, оскільки я бачу, що з Вашого рахунку була зроблена спроба здійснити транзакцію на рахунок XXX, який знаходиться в нашій системі в чорному списку. Будь ласка, назвіть свій ПАРОЛЬ...

Я працівник технічного відділу і телефоную Вам, тому що Ваші рахунки були заблоковані. Для того, щоб їх розблокувати, я зателефоную Вам за кілька хвилин і Ви увійдете до свого облікового запису при мені.

Злочинці крадуть Ваші гроші, зокрема, шляхом зняття заощаджень з банківського рахунку, проведення карткових операцій або отримання позики/кредиту з використанням Ваших персональних даних.

Як захиститися, щоб не втратити гроші?
Слід дотримуватися кількох важливих правил:

1. не повідомляйте свої логін та пароль до інтернет-банкінгу, реквізити платіжної картки (номер картки, CVV-код, термін дії, ПІБ власника) - справжній представник банку ніколи про це не попросить;
2. ніколи не розголошуйте коди до інтернет-банкінгу, коди BLIK або коди 3D Secure, які надходять на Ваш телефон і використовуються для підтвердження переказів або інших платежів, включаючи онлайн-транзакції картками;
3. завжди читайте зміст текстових повідомлень (SMS), які приходять на Ваш телефон, або повідомлень у мобільному додатку банку. Їх зміст може означати, що Ви погоджуєтеся на транзакцію, здійснену злочинцями;
4. читайте зміст повідомлень, які Ви отримуєте кожного разу, особливо під час розмови з начебто консультантом. Їх зміст може свідчити про те, що Ви додаєте до свого профілю (рахунку в електронному банкінгу) НОВИЙ ДОВІРЕНИЙ пристрій, за допомогою якого шахраї викрадуть Ваші гроші або візьмуть позику/кредит.

Якщо розмова викликає занепокоєння або сумніви:
припиніть розмову, зачекайте мінімум 30 секунд. Потім зателефонуйте до банку чи установи, представник якої телефонував. Обов'язково набирайте офіційний номер на клавіатурі, не передзвонюйте на номер зі списку останніх дзвінків, який відображається на Вашому телефоні.

- керуйтеся здоровим глуздом та зберігайте холодну голову! Навіть якщо Вам повідомили про потенційну загрозу, наприклад, втрату заощаджень, спокійно подумайте, чи дійсно Ваші гроші можуть опинитися в небезпеці? Можливо, Ви розмовляєте з шахраєм? Перервіть розмову та зателефонуйте до свого банку, як описано вище;
- пам'ятайте, що відображений на екрані номер телефону або назва банку не є гарантією того, що Ви розмовляєте з правдивим представником банку;
- Ви завжди можете повідомити про свої підозри до свого банку, а в разі скоєння злочину - також повідомити поліцію.

FinCERT.pl – Банківський центр кібербезпеки Асоціації польських банків - Центр обміну та аналізу інформації фінансового сектору

Центральне бюро по боротьбі з кіберзлочинністю

Головне управління поліції

_____

FinCERT.pl - Банківський центр кібербезпеки Асоціації польських банків - оперативний підрозділ, що діє в рамках Групи безпеки банків Асоціації польських банків, яка збирає, аналізує та передає, в межах банківського сектору та у співпраці з правоохоронними органами та іншими установами, інформацію про можливі загрози та інциденти злочинного характеру, що загрожують безпеці банків або їхніх клієнтів.