Мошенники звонят с номеров, выдающих себя за банки или другие учреждения общественного доверия

- Сообщение от FinCERT.pl – Банкосвкого центра кибербезопасности Союза польских банков Центрального управления по борьбе с киберпреступностью Главного отделения полиции от 7 декабря 2022 года

Спуфинг, т.е. ложные телефонные звонки преступников, выдающих себя за банки или другие учреждения общественного доверия, такие как Союз польских банков, Управление финансового надзора, ...!

Остерегайтесь телефонных звонков, в которых мошенники выдают себя за работника банка или другое заслуживающее доверия лицо (например, работника Управления финансового надзора, работника Группы банковской безопасности Союза польских банков или сотрудника полиции). Во время ложного звонка на Вашем телефоне может появиться Ваш номер телефона или название надежного учреждения.

Преступник будет воздействовать на Ваши эмоции, чтобы ввести Вас в состояние ощущения угрозы, беспокойства, тревоги или любопытства. Мошенник будет говорить с вами на украинском, русском, изредка польском языках.

Цель - получить конфиденциальную информацию (логин и пароль для входа в электронную банковскую систему, BLIK-коды, данные платежных карт) или убедить Вас выполнить определенные действия (например, установить приложение, которое предоставляет преступникам удаленный доступ к вашему компьютеру или телефону).
Ниже приведены примеры разговоров:

Добрый день, подтверждаете ли Вы перевод на сумму 800 злотых для г-на Дариуша? ... Нет? Тогда мы должны быстро заблокировать его. Пожалуйста, установите приложение XXX, и я помогу вам решить эту проблему.

Здравствуйте, я работник банка и связываюсь с Вами, потому что вижу, что была предпринята попытка провести операцию с Вашего счета на счет XXX, который находится в черном списке нашей системы. Пожалуйста, сообщите мне ваш ПАРОЛЬ ...

Я работник технического отдела и звоню Вам, потому что Ваши средства были заблокированы. Чтобы разблокировать их, я позвоню Вам через несколько минут, и Вы войдете в свой аккаунт вместе со мной.

Преступники крадут Ваши деньги, в частности, путем вывода сбережений с Вашего банковского счета, совершения операций с помощью банковских карт или получения займа/кредита, используя Ваши личные данные.

Как защитить себя, чтобы не потерять деньги?
Следует соблюдать несколько важных правил:

1. не сообщайте логин и пароль для входа в электронную банковскую систему, данные платежной карты (номер карты, CVV, срок действия, имя и фамилию владельца карты) - настоящий представитель банка никогда не спросит об этом;
2. никогда не сообщайте входящие на Ваш телефон коды для электронной банковской системы, BLIK-коды или коды 3D Secure, используемые для подтверждения переводов или других платежей, включая операции с использованием банковских карт в Интернете;
3. всегда читайте содержание SMS-сообщений, входящих на Ваш телефон, или сообщений в мобильном приложении банка. Их содержание может указывать на то, что вы соглашаетесь на операцию, которую осуществляют преступники;
4. каждый раз читайте содержание уведомлений, которые Вы получаете, особенно во время текущего разговора с предполагаемым консультантом. Их содержание может указывать на то, что вы добавляете в свой профиль (в аккаунте электронной банковской системы) НОВОЕ НАДЕЖНОЕ устройство, с помощью которого мошенники украдут у Вас деньги или возьмут займ/кредит.

Если в ходе разговора возникли опасения или сомнения:
положите трубку, подождите не менее 30 секунд. Затем соединитесь с банком или учреждением, представитель которого Вам звонил. Обязательно наберите официальный номер на клавиатуре, не перезванивайте из списка вызовов, который появляется на экране Вашего телефона.

- сохраняйте здравый смысл и холодную голову! Даже если Вы были проинформированы о возможной угрозе, например, о потере средств, спокойно подумайте, действительно ли средствам может угрожать опасность? Может быть, Вы все-таки разговариваете с мошенником? Прервите звонок и свяжитесь с банком в соответствии с вышеизложенным;
- помните, что указанный номер телефона или название банка не являются гарантией того, что Вы разговариваете с настоящим представителем банка;
- Вы всегда можете сообщить о своих подозрениях в банк и, если было совершено преступление, также сообщить об этом в полицию.

FinCERT.pl - Банковский центр кибербезопасности Союза польских банков - Центр обмена и анализа информации финансового сектора

Центральное управление по борьбе с киберпреступностью

Главное отделение полиции

FinCERT.pl - Банковский центр кибербезопасности Союза польских банков - оперативное подразделение, действующее в рамках Группы банковской безопасности Союза польских банков, которое собирает, анализирует и передает в рамках банковского сектора и в сотрудничестве с правоохранительными органами и другими учреждениями информацию о возможных угрозах, а также об инцидентах преступного характера, которые ставят под угрозу безопасность банков или их клиентов.