ВНИМАНИЕ: ОПАСНОСТЬ

Новые способы мошенничества

Телефонные мошенники изобрели новый способ обмана клиентов российских банков, отмечает «Российская газета». Грабители сообщают клиенту банка о попытке вывести средства со счета в другом регионе

«Недавно на экране моего мобильного телефона высветился входящий городской вызов. Собеседник обратился по имени и представился сотрудником банка. Этот человек сказал, что его звонок – попытка помочь мне. Так как банку стала очевидна несанкционная попытка перевода моих денежных средств в другом регионе», – вспоминает одна из жертв. Банк якобы видит транзакции в основном на территории одной области, а попытка списания средств происходит в другой. Когда клиент сообщает, что не совершал данную операцию, мошенники говорят, что банк блокирует процедуру, после чего предлагают в целях безопасности назвать устройства, с которых клиент входит в личный кабинет.

Обманутые клиенты банков подчеркивают, что они не самые доверчивые люди и что «сотрудник банка» не запрашивал у них никаких конфиденциальных данных, тем самым долго не вызывал подозрения.

Отключить операционку

Но для того чтобы полностью обеспечить безопасность счетов, «сотрудник» предложил сверить устройства, имеющие доступ к личному кабинету. Ключевым моментом в диалоге стала сверка операционной системы Android и IOS.

Когда становится известно, какой операционной системой пользуется человек, мошенники предлагают отключить лишнюю ОС с помощью программы teamviewer.

Программа делегирования доступом teamviewer позволяет подключиться к смартфону постороннему человеку и совершить любую операцию от вашего лица. Для подключения у вас запросят id (специальный номер) пользователя, сообщив который, третья сторона легко подключится и завладеет конфиденциальной информацией смартфона. В данном случае доказать попытку несанкционного взлома будет крайне сложно или вообще невозможно. Ведь вы добровольно предоставили доступ.

Звонок от «представителя банка» – самая распространенная схема, которой пользуются аферисты, чтобы получить доступ к чужим кредитным и дебетовым картам.

На днях телефонные мошенники установили антирекорд – с карты москвича по такой схеме сняли 3,5 млн рублей, сообщает РИА «Новости».

Аферисты нередко мимикрируют под сотрудников службы безопасности банка. Они знают не только паспортные данные, но и для убедительности могут сообщить ваш остаток на счете, банкомат, в котором вы в последний раз снимали деньги. И вы им верите.

Многие пострадавшие от мошенников вспоминают, что во время разговора на заднем плане бывают слышны звуки call-центра, просьбы «оставаться на линии» или «оценить работу оператора».

Еще один способ развода – «Пройдите биометрическую идентификацию по телефону». Это классический сценарий обмана. Есть и другие.

Например, аферисты представляются «сотрудниками правительства» вашего региона. Они могут обратиться к жертве по имени-отчеству и обрадовать сообщением о причитающейся компенсации. Далее мошенники просят продиктовать номер карты для перевода «компенсации», а также назвать код с обратной стороны карты.

Без антивируса – без денег

Ранее в июле эксперты по кибербезопасности предупредили еще об одном способе хищения денег с банковских карт: злоумышленники заражают сайты специальной программой-скиммером с помощью JavaScript.

В блоге компании Sucuri появилась информация о новом способе мошенничества с банковскими картами. К сотрудникам бренда обратился владелец веб-сайта, чей ресурс неожиданно оказался в черном списке антивируса. Как оказалось, он был заражен программой-скиммером, нацеленной на кражу денежных средств с карт пользователей.

Оказалось, что скиммер был связан с доменом google-analyt cs[.]com, который относится к интернационализованным доменным именам – как можно заметить, в адресе есть буква национального алфавита. Заменяя одну букву на другую, злоумышленник обманом завлекает пользователя на поддельный сайт, отличающийся от оригинала на один символ. Кроме того, «google» в адресе наталкивает юзера на мысль, что это надежный сайт, и усыпляет его бдительность.

Когда пользователь заходит на фейковый сайт, скиммер незаметно для владельца карты похищает передаваемые им данные, отправляя их оператору-злоумышленнику.

По словам начальника отдела по противодействию мошенничеству Центра прикладных систем безопасности компании «Инфосистемы Джет» Алексея Сизова, «количество сайтов-двойников, случаев инъекций опасного кода на web-ресурсы имеет лавинный рост». «Механизмы противодействия таким атакам существуют, но далеко не все ресурсы обеспечивают контроль за инъекциями, особенно когда они проводятся на устройстве клиента. Далеко не все сайты-клоны обнаруживаются и блокируются оперативно», – добавляет он.

Киберпреступники могут взламывать сайты, используя атаки «грубой силой» или же утечку учетных данных, чтобы внедрить вредоносный код. В данном случае они использовали JavaScript – с его помощью захватываются данные платежа, введенные на сайт, рассказал «Газете.Ru» ИБ-евангелист компании Avast Луис Корронс.

Подобные методы особенно страшны для пользователей, у которых на устройстве, используемом для доступа к сайту, не установлен антивирус.

По материалам Газета.ru

ПРИМИТЕ К СВЕДЕНИЮ

10 «ценных» вещей, которые немедленно надо выбросить

1. Косметика с истекшим сроком годности. Вот зачем хранить старую тушь и помаду? А собирать пустые флаконы из-под духов? Любая косметика создана, чтобы делать нас красивее, а не вызывать бактериальную инфекцию.

2. Неудобная обувь. Признайся, есть же такие туфли, надевая которые, каждый раз проклинаешь их из-за невыносимых болей и мозолей?! Не можешь выбросить такие туфли? Поставь их на самое видное место и подпиши: «Мое любимое орудие пыток».

3. Одежда «Когда я похудею». Где-то в дальнем углу шкафа лежит аккуратная стопочка вещей, которые ты мечтаешь надеть, когда сбросишь лишние килограммы. Да, это работает как мотивация, но негативная и удручающая.

4. Открытки от людей, которых не помнишь. В маленькой коробочке хранится стопка поздравительных открыток. От людей, с которыми ты уже никогда не будешь общаться. Зачем нужен этот склад из картонок с «искренними» пожеланиями? Оставь открытки только от близких, остальное – в мусор!

5. Фарфоровая посуда. Музейные экспонаты должны храниться в музее! Поставь на место фарфора вазоны с живыми цветами – больше никакого нафталина.

6. Бумажный спам. Зачем тащить в квартиру разную печатную продукцию из почтового ящика? Единственное, что нужно, – счета за коммунальные услуги.

7. «Неносибельное» нижнее белье. Кто придумал классификацию белья «на критические дни», «на каждый день» и «по особому случаю»? Проведи ревизию и оставь только трусики и лифчики, в которых чувствуешь себя особенно сексуально. И выбрось все колготки со стрелками с таинственной миссией «Под штаны» (никогда же их не наденешь!).

8. Старые телефоны, плееры и прочую технику. Эти ценные гаджеты могут пригодиться юным физикам-испытателям для опытов, но тебе они абсолютно не нужны.

9. Книги, которые никогда не прочитаешь. На видном месте должны стоять только любимые книги и те, которые нужны по работе/учебе.

10. Воспоминания о бывших отношениях. Не можешь выбросить футболку бывшего, которая до сих пор пахнет его духами? Или стопку рукописных стихов, написанных изменником только для тебя? Избавившись от материальных напоминаний, легче выкинешь и человека из головы.

Ну что, начнем?

АНГЕЛ
www.pamyatniki.ru

Вспольинское поле, 2
Пр-т Октября, 96а
т.:(4852) 21-07-75

до 31 августа

Памятник
с установкой

- 15%

Реклама

*Срок действия предложения с 15.07.2019 г. по 31.08.2019 г.
Подробности уточняйте по адресу г. Ярославль, ул. Вспольинское поле,2 и по телефону (4852) 21-07-75