Приложение

ИНФОРМАЦИЯ
о способах совершения мошенничеств и методах защиты от них

1. Мошенничества с платежными картами
Звонки и сообщения из банков через виртуальные АТС

Этот способ мошенничества является наиболее новым. Злоумышленники оформляют облачную АТС на одноразовую сим-карту, а затем через веб-интерфейс меняют телефонный номер своей станции на телефонный номер банка. Представляясь сотрудниками банка, преступники обзванивают клиентов и под различными предлогами выясняют у них номера карт, одноразовые пароли и коды доступа, необходимые для проведения операций по банковским картам. Также с номера-двойника банка мошенники массово рассылают клиентам банка смс-сообщения о блокировке карты. Для разблокировки им предлагают перевести деньги на счет или отправить смс-сообщение на короткий номер.

Фишинг

Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к аккаунтам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Для кражи персональных данных фишеры массово рассылают электронные письма от имени государственных органов или известных компаний, например, крупных банков или онлайн-магазинов. Их цель - заставить получателей перейти по указанной в письме ссылке на поддельный сайт компании, интерфейс которого внешне не отличим от настоящего сайта, и ввести свои личные данные. Для привлечения внимания к письму в теме указывается на перспективу большой выгоды или на проблему, требующую срочного разрешения.

Подставные страницы действуют недолго - как правило, не более одной недели, ввиду частого обновления базы антифишинговых программ и фильтров. Однако мошенники, следуя отлаженной схеме, создают всё новые и новые сайты-фальшивки для сбора персональных данных.

Так, спамеры активно рассылали по всему миру фальшивые уведомления о выигрыше в лотереях, приуроченных к Чемпионату Европы по футболу, Олимпиаде в Бразилии и Чемпионатам мира по футболу в 2018 и 2022 годах. Для получения денег получателю письма предлагалось ввести на сайте несуществующей лотереи персональную информацию.

Жители России получали письма, замаскированные под уведомления от Федеральной налоговой службы и Пенсионного фонда РФ, примерно

следующего содержания: «Уважаемый налогоплательщик! У вас выявлена задолженность. Срок погашения долга до 23.12.2016 г. Подробнее Вы можете ознакомиться, перейдя по ссылке… » или «Осуществлен перерасчет пенсионных накоплений. Обязательно ознакомьтесь по ссылке…». После перехода на поддельный сайт государственного органа для получения более подробной информации пользователю предлагалось ввести свои персональные данные.

Скимминг

Считывание данных карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру.
Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты.

2. Совершение покупок в сети Интернет

Мошенники привлекают потенциальных жертв низкими ценами на товары известных брендов. Покупателей просят внести предоплату, как правило, перевести денежные средства на электронный кошелек. В течение нескольких дней магазин обещает скорую доставку товара, после чего бесследно исчезает.
Схожий способ мошенничества используется при продаже товаров или услуг на электронных досках объявлений, интернет-аукционах, форумах, сервисах бронирования недвижимости. Как и в случае с интернет-магазинами, мошенники привлекают своих жертв низкими ценами и требуют перечисления предоплаты на электронный кошелек или банковскую карту.

Оформление полиса ОСАГО

Мошенники регистрируют доменное имя, содержащее в названии слово «osago» или напоминающее доменное имя одной из известных страховых компаний. На этом домене размещается фишинговый сайт, страницы которого практически полностью копируют оформление оригинального веб-ресурса, принадлежащего страховой компании. Для расчета стоимости страхования пользователю необходимо заполнить небольшую анкету - указать имя, дату рождения, номер водительского удостоверения, данные об автомобиле, номер телефона и электронную почту для связи. После введения данных покупателю предлагают оплатить электронный полис ОСАГО с помощью банковской карты: указать номер карты, дату окончания ее действия и CVC/CVV-код. Мошенники перенаправляют пользователя на поддельную страницу подтверждения оплаты, где просят ввести полученный от банка код подтверждения оплаты. В случае успеха злоумышленники обходят двухфакторную аутентификацию и получают деньги.

Аналогичную схему обмана можно встретить при покупке авиабилетов онлайн.

3. Выигрыш в лотерею

С помощью массовой рассылки электронных писем и смс-сообщений мошенники оповещают потенциальных жертв о выигрыше ценных призов. Для их получения злоумышленники просят перевести на электронные счета некоторую сумму денег, объясняя это необходимостью уплаты налогов, таможенных пошлин или транспортных расходов.

4. Мошенничества под предлогом благотворительности

Мошенники размещают в социальных сетях или на форумах подложные объявления о сборе средств тяжелобольным детям или бездомным животным или делают репосты реальных объявлений, но с подложными банковскими реквизитами.

5. Мошенничества, направленные на заражение устройства пользователя вредоносной программой

Мошенники, используя электронные адреса, схожие с адресами легальных организаций, рассылают от их имени сообщения, содержащие ссылку на скачивание открытки, музыки, картинки, архива или программы. Запуск вложения или переход по ссылке может инициализировать установку на устройство вредоносносной программы (вымогателя-блокиратора, шифровальщика, троянской программы) или же оформление подписки на платную услугу.

Общие рекомендации по обеспечению безопасной работы в сети Интернет

- никому не передавать конфиденциальные данные (логин, пароль), в том числе родственникам, коллегам;
- использовать сложные пароли, состоящие из букв, цифр и специальных символов, исключить использование паролей по умолчанию, (второй год подряд самым популярным паролем в мире является «123456»);
- регулярно осуществлять смену паролей, обеспечить их конфиденциальность;
- использовать в работе лицензионное программное обеспечение с установленными обновлениями безопасности;
- на всех устройствах, должно быть установлено лицензионное антивирусное программное обеспечение с актуальными обновлениями;
- не использовать общественные беспроводные сети и устройства для работы с личной информацией;

- не использовать программные продукты, полученные из сомнительных источников (пиринговые и файлообменные сети), модифицированные программные продукты, не посещать ресурсы с сомнительной репутацией;

- личную информацию вводить только при безопасном соединении (URL веб-сайт должен начинаться с «https://», в интерфейсе браузера должна появиться иконка замка);

- выполнять резервное копирование важной информации.

Чтобы не стать жертвой злоумышленников при пользовании банковскими картами необходимо придерживаться следующих правил:

- никому не сообщать пин-, CVC- или CVV- коды банковской карты и одноразовые пароли;

- в торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты. В противном случае мошенники могут получить реквизиты карты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки;

- в случае потери банковской карты немедленно позвонить в банк для блокировки - это поможет сохранить денежные средства;

- подключить услугу смс-информирование - это обеспечит контроль за проведением любых операции по карте. При получении смс о несанкционированном списании средств со счета, заблокировать карту;

- установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удалённо - в интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте;

- при вводе пин-кода прикрывать клавиатуру. Вводить пин-код быстрыми отработанными движениями - это поможет в случае, установки скрытых видеокамер мошенников;

- выбирать для пользования терминалы и банкоматы, которые расположены непосредственно в отделениях банка или других охраняемых учреждениях;

- использовать банковскую карту в торговых точках, не вызывающих подозрений;

- перед тем как вставить карту в картоприемник внимательно осмотреть банкомат на предмет наличия подозрительных устройств, проверить, надежно ли они закреплены. Если очевидно, что накладное устройство смонтировано кустарно (можно увидеть остатки клея, ненадежность конструкции и неравномерность крепления), то необходимо позвонить на горячую линию банка, сообщить о данном факте и воспользоваться другим банкоматом;

- в случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - рекомендуется отказаться от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.