НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU

БАНКОМАТЫ: СКИММЕРЫ И ШИММЕРЫ

БАНКОМАТЫ: СКИММЕРЫ И ШИММЕРЫ

Наличные деньги постепенно уходят из повседневной жизни, но все же нам по-прежнему приходится взаимодействовать с банкоматами. Несмотря на то что ваша банковская карта защищена сразу несколькими технологиями, шанс потерять с нее все средства остается. Чтобы этого не произошло – проявляйте должную бдительность.

Одним из способов воровства денег с карт является скимминг*. Основой данного способа является монтирование на щель картоприемника банкомата специальной «накладки», которая считывает магнитную ленту банковской карты и пересылает данные хозяину устройства. Как правило, такие накладки используются в паре со скрытой камерой, направленной на клавиатуру для ввода пин-кода.

В российских условиях скимминг практически не прижился в силу низкой распространенности терминалов оплаты, использующих магнитную ленту, и в целом использования более продвинутых моделей банкоматов. Несмотря на это, рекомендуем всякий раз проверять банкомат по следующим параметрам:

- проверьте картоприемник на наличие «накладки»: попробуйте его «оторвать»;
- проверьте все выступающие панели – фальшивые плохо держатся;
- если клавиатура кажется вам избыточно «выпуклой» или отличающейся по цвету/тону – попробуйте ее поддеть. Не стесняйтесь проверять панели банкомата!

В последние годы набирает обороты более продвинутая технология с использованием шиммера**. Шиммер устанавливается внутрь картоприемника, и снаружи его обнаружить невозможно. До сих пор использование шиммеров было не слишком распространено в силу дороговизны изготовления устройства и высоких рисках быть замеченным при его установке в банкомат.

Несмотря на это, стоит следовать следующим правилам:

- по возможности не пользуйтесь картоприемником – все современные банкоматы позволяют использовать карту бесконтактно;
- избегайте банкоматы, установленные на улице, старайтесь пользоваться теми, что находятся под постоянным наблюдением.

***Скимминг** (от англ. skim - быстро читать) – метод кражи данных банковской карты с использованием специальных технических устройств, несанкционированно вмонтированных в банкомат.

****Шиммер** (от англ. shim - клин, тонкая прокладка) – это тонкая «прокладка», которая располагается между чипом на карте и считывающим устройством чипов в банкомат или терминале – и записывает данные с чипа, когда их считывает терминал.

НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU

ИСПОЛЬЗОВАНИЕ ПУБЛИЧНЫХ WI-FI СЕТЕЙ

Использование публичных Wi-fi сетей

Все больше общественных мест, кафе и транспорта открывает в публичный доступ свои Wi-Fi сети. Часто для выхода для бесплатного Wi-Fi даже не нужен пароль. Несомненно, это удобно для пользователей, но каждая такая точка доступа является потенциальным источником «цифровой инфекции».

Киберпреступники давно научились эксплуатировать подобные публичные Wi-Fi для достижения своих целей: собирать логины и пароли, а также другие личные данные в общественных местах можно в «промышленных масштабах».

ПРОЯВЛЯЙТЕ ДОЛЖНУЮ БДИТЕЛЬНОСТЬ:

1. Не доверяйте точкам доступа в интернет, которые не закрыты паролем.

Чаще всего именно такие сети используют для воровства конфиденциальных данных пользователей.

2. Выключайте Wi-Fi, если вы им не планируете пользоваться.

Во-первых, это сэкономит заряд батареи. Во-вторых, не позволит следить за вами: включенный модуль Wi-Fi периодически отправляет в «эфир» свои идентификационные данные (MAC-адрес). Таким образом вполне можно составить маршрут вашего передвижения. Как правило, подобный прием используют крупные компании для внутренних исследований с целью повышения маркетинговых мероприятий. Но данная информация может использоваться злоумышленниками.

3. Отключите функцию автоматического подключения к Wi-Fi на телефоне и планшете.

Преступник легко создаст «клон» реальной публичной точки доступа для того, чтобы собирать данные пользователей, подключившихся автоматически.

4. Не заходите в интернет-банк.

В прошлом номере вы касались темы «фишинга». В случае использования публичного Wi-Fi вам не удастся определить фишинговый сайт по неправильному написанию адреса сайта: злоумышленник может перенаправить обращение к реальному сайту и подставить данные со своего сервера. В таком случае по визуальным признакам будет невозможно понять, что вас ввели в заблуждение.

5. По возможности используйте VPN.

Это хороший способ не только защитить передаваемые через интернет данные, но и в целом анонимизировать ваше нахождение в сети.

ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

НЕФТЕГАЗСТРОЙПРОФСОЮЗ РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU

ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Любой программный продукт требует периодического обновления. Чем популярнее программа, тем больше число злоумышленников, систематически работающих над поиском уязвимостей в ней.

Следует понимать, что невозможно написать идеально защищенную программу, особенно в текущих реалиях: подавляющее большинство ПО не обладает изолированным кодом и постоянно взаимодействует со сторонними сервисами для обмена данными. Каждая подобная «точка входа» является потенциальной уязвимостью.

В КАЧЕСТВЕ ПРОФИЛАКТИКИ ВЫПОЛНЯЙТЕ СЛЕДУЮЩИЕ РЕКОМЕНДАЦИИ:

- без необходимости не производите на телефоне Rooting (Android), Jailbreak (Apple iOS), HardSPL (Windows Phone)*;
- обновляйте мобильные приложения по мере получения уведомлений от разработчика;
- при обновлении программ на компьютере/ноутбуке пользуйтесь автоматическим обновлением или загружайте обновления только с сайта производителя;
- периодически обновляйте прошивку на вашем роутере;
- не забывайте об обновлении «умных устройств» (умные колонки, бытовая техника и устройства с выходом в интернет);
- при необходимости обновления специализированных/прикладных программ (например, 1С Предприятие) обязательно предварительно проконсультируйтесь с IT-специалистом.

*** Rooting / Jailbreak / HardSPL –** процесс получения прав суперпользователя на устройствах. Основными целями являются снятие ограничений производителя либо оператора связи, манипулирование системными приложениями и возможность запуска приложений, требующих прав администратора.

НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU

«ПИРАТСКОЕ» ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«ПИРАТСКОЕ» ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

В связи с уходом ряда ведущих поставщиков ПО с российского рынка возникает соблазн использования «ломаного софта».

Зачастую именно такие продукты являются источником заражения операционной системы.

Необходимо понимать, что нередко в комплексе с «кряком» пользователь, не осознавая того, своими руками устанавливает вредоносное ПО и предоставляет ему полные права, исключая из сканирования антивирусом.

Не обязательно негативное воздействие будет проявляться сразу после попадания в систему.

Злоумышленник в состоянии настроить работу программы таким образом, что пользователь долгое время не сможет распознать заражение.
За время скрытого нахождения в системе программа злоумышленника соберет достаточно информации, чтобы при единовременной передаче данных снабдить создателя всем необходимым для нанесения максимального ущерба.

В целом даже без получения платежных реквизитов банковских карт злоумышленник в силах «монетизировать» полученную информацию.

Например:

Идентифицировав жертву и получив доступ к аккаунтам социальных сетей, возможно инициировать сбор денежных средств для якобы находящихся в тяжелом состоянии родственников.

Сопроводив данные посты сканами реальных паспортов и используя другую конфиденциальную информацию, злоумышленник проведет «идеальную» атаку.

Фактически вариантов подобных атак – бесконечное множество.

Без крайней необходимости НИКОГДА не используйте взломанные версии лицензионного программного обеспечения.

ФИШИНГ

НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU

ФИШИНГ

Поскольку фишинг* базируется на социальной инженерии, защита от него ложится в основном на обычного пользователя. Действия злоумышленника направлены на побуждение пользователя к самостоятельной передаче необходимых данных на поддельной странице.

Как защититься:

1. Ставьте под сомнение каждое письмо с почтовыми вложениями и ссылками: перед переходом по ссылке и открытии вложения удостоверьтесь, что письмо пришло от ожидаемого отправителя.

Также посимвольно проверьте домен ссылки из письма: мошенники часто используют «похожие» адреса типа «odnoklsssniki.ru».

2. Разделите почтовые ящики:

a) Отдельный email для подписок, акций и регистрации в интернет-магазинах;

b) Личный ящик для важных и личных писем;

c) Не используйте рабочий email для регистрации без крайней необходимости.

Таким образом вы заведомо отделите потенциально опасные письма.

3. Вместо перехода по ссылке из письма – введите веб-адрес в адресную строку браузера самостоятельно.

4. Не переходите по подозрительным ссылкам, которые также распространяются через соцсети и мессенджеры.

5. Не спешите реагировать на письма с «провокационными» заголовками. Зачастую, чтобы гарантированно привлечь внимание пользователя, «фишеры» используют заголовки типа «Подтверждение списания с банковского счета» или «Начисление штрафа за неуплату налогов».

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Подозрительны любые письма, не содержащие какой-либо конкретной личной информации.

Проанализируйте, есть ли предпосылки для получения подобных писем. Свяжитесь с организацией, от имени которой пришло письмо, по номеру телефона из альтернативного источника (например: Яндекс.Карты).

***Фишинг** — вид кибермошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам и паролям, платежным реквизитам банковских карт.