



ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА РЕСПУБЛИКИ АЛТАЙ

**ПРОКУРАТУРА
УСТЬ-КАНСКОГО РАЙОНА**

ул. Лесная, 8
с. Усть-Кан, Республика Алтай,
Россия, 649450



Главе МО «Усть-Канский район»,
а также главам сельских поселений

25.12.2024 № 22/2-04-2024/289-24-20840009

На № _____

ИНФОРМАЦИЯ

на сайты муниципальных
образований

В целях профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий, предупреждения совершения преступлений данной категории сообщаем о новых способах, используемых мошенниками.

Мошенники начали применять новую схему для кражи денег россиян: в ней задействованы виртуальные клоны банковских карт, которые создаются при помощи шпионского софта.

В схеме скомбинированы две стратегии: социальная инженерия и шпионские программы. Цель — украсть данные карты клиента, сделать ее клон и расплачиваться в магазинах через терминалы.

Злоумышленники звонят потенциальной жертве, представляясь сотрудниками сотового оператора, и сообщают о необходимости продлить договор на обслуживание. Для этого клиента просят установить мобильное приложение оператора. Могут использоваться и другие предлоги, например обновление антивируса, приложения медицинских сервисов и прочее.

На самом деле это вредоносное ПО — шпионская программа. Она позволяет злоумышленникам удаленно управлять устройством, включая камеру, микрофон и функции NFC.

После того как владелец смартфона установит приложение, мошенники под предлогом подтверждения данных для продления договора дают инструкцию: жертву просят сфотографировать карту или поднести к смартфону, а затем ввести старый ПИН-код и якобы сменить его на новый (на самом деле смена ПИН-кода не происходит).

В это время с помощью шпионской программы злоумышленники активируют NFC на устройстве жертвы. Параллельно другая программа, уже на смартфоне мошенника, используется для перехвата данных карты (ID, срок действия). Полученные данные привязываются к устройству злоумышленников.

Такой виртуальный клон карты позволяет им снимать деньги в банкоматах и совершать бесконтактные платежи в магазинах с NFC-терминалами.

Чтобы не попасться на уловки мошенников, не устанавливайте приложения по ссылкам, присланным через мессенджеры. Приложения операторов, торговых сетей, медицинских компаний можно скачать на их официальных сайтах. Установка приложений со стороны может нести риск хищения средств со счетов.

Будьте внимательны и не поддавайтесь на уловки мошенников!

Прокурор района

Н.А. Мунатов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 0084AC9267FAF453FE2D456819B4BF50E4

Владелец Мунатов Никита Андреевич

Действителен с 16.04.2024 по 10.07.2025



ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА РЕСПУБЛИКИ АЛТАЙ

**ПРОКУРАТУРА
УСТЬ-КАНСКОГО РАЙОНА**

ул. Лесная, 8
с. Усть-Кан, Республика Алтай,
Россия, 649450



444639 925300

Главе МО «Усть-Канский район»,
а также главам сельских поселений

25.12.2024 № 22/2-04-2024/290-24-20840009

На № _____

ИНФОРМАЦИЯ

на сайты муниципальных
образований

В целях профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий, предупреждения совершения преступлений данной категории сообщаем о новых способах, используемых мошенниками.

Пользователи могут менять сотовых операторов и подключать новые сим-карты. Часто бывает, что старый номер остается привязан к какому-то аккаунту: на «Госуслугах», в интернет-банке или в соцсетях. Одни пользователи при подключении новой сим-карты переводят на нее все учетные записи. Другие оставляют всё как есть: личный кабинет, так и остается привязанным к старому номеру. На такие симки и охотятся мошенники в надежде получить доступ к персональным данным.

Как действуют мошенники

Взлом аккаунта выглядит следующим образом:

1. Преступники сверяют номера, которые есть в открытой продаже, с теми, которые привязаны к каким-либо личным кабинетам.

Затем покупают у сотовых операторов те номера телефонов, которые давно не используются владельцами, но раньше были привязаны к какому-то цифровому сервису.

2. С помощью сим-карт злоумышленники пытаются взломать личный кабинет банка, «Госуслуг» или другого онлайн-сервиса. Если вы не меняли настройки, то аккаунт так и остается привязанным к старому контакту.

3. Войти в учетную запись не составляет труда: на телефон приходит одноразовый пароль для входа. Поэтому телефонный номер важно беречь: это не просто комбинация цифр для связи, а важный код доступа к личному кабинету, один из этапов авторизации.

4. Получив доступ к личному кабинету, мошенник может совершить от вашего имени любые действия.

Даже если на счете нет денег, и вы давно не пользуетесь услугами этого банка, мошенники все равно смогут совершить преступление - например, оформить кредит. Бывает, что банк выдает кредит на имя клиента, который когда-то оставлял данные и в истории банка числится как подходящий под условия выдачи займа.

Тем более что на рынке разрешены программы без подтверждения дохода, если клиент ранее уже предоставлял банку свои данные. Таким образом, вы можете узнать о наличии кредита только спустя несколько месяцев.

Будьте внимательны и не поддавайтесь на уловки мошенников!

Прокурор района

Н.А. Мунатов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 0084AC9267FAF453FE2D456819B4BF50E4

Владелец **Мунатов Никита Андреевич**

Действителен с 16.04.2024 по 10.07.2025



ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА РЕСПУБЛИКИ АЛТАЙ

**ПРОКУРАТУРА
УСТЬ-КАНСКОГО РАЙОНА**

ул. Лесная, 8
с. Усть-Кан, Республика Алтай,
Россия, 649450



Главе МО «Усть-Канский район»,
а также главам сельских поселений

25.12.2024 № 22/2-04-2024/291-24-20840009

На № _____

ИНФОРМАЦИЯ

на сайты муниципальных
образований

В целях профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий, предупреждения совершения преступлений данной категории сообщаем о новых способах, используемых мошенниками.

Что такое спуфинг?

Спуфинг (от английского spoof – обман, подделка) – это кибератака, при которой мошенники маскируются под других людей или компании.

Ее целью является завоевать доверие жертвы, чтобы получить доступ к устройствам, украсть деньги, личные данные или распространить вирусные программы.

Следуя этой схеме, злоумышленники создают фальшивые номера, сайты и рассылки, маскируя их под известные источники.

Целью спуфинга является попытка получить доступ к устройствам граждан, распространить вирусные программы и получить личные данные пользователей.

Типы спуфинга.

Самые простые – это подмена номера телефона, адреса электронной почты или сайта. К более сложным относят IP-спуфинг, ARP-спуфинг и DNS-спуфинг.

Среди наиболее распространенных типов спуфинга:

- Спуфинг с подменой адреса электронной почты. Мошенники подделывают заголовки электронной почты и просят адресата перевести им деньги или открыть доступ к системе. Сообщения могут содержать вложения: стоит только их открыть, как на устройство пользователя устанавливается вредоносная программа;

- Спуфинг с подменой сайта или URL-адреса. Злоумышленник создает фальшивый сайт, который практически неотличим от настоящего, для кражи учетных данных. Иногда заражают устройство вредоносным ПО;

- Спуфинг с подменой номера вызывающего абонента. На экране телефона отображаются ложные сведения о вызывающем абоненте – люди охотнее отвечают на звонки с местных номеров, чем с незнакомых. Для подмены данных используется технология VoIP (IP-телефония), которая позволяет злоумышленникам самостоятельно выбрать номер и указать нужные им сведения о звонящем. Во время разговора с жертвой они пытаются выяснить личную информацию;

- SMS-спуфинг. Тип атаки, при которой аферист использует ложные сведения об отправителе сообщения. Как правило, мошенники прячутся за номер какой-то известной компании. В сообщении – ссылки на фишинговые сайты и вредоносные программы;

- IP-спуфинг. Подмена IP-адреса нацелена не на конкретного пользователя, а преимущественно на сетевые технологии. Злоумышленники заменяют заголовки пакетов, используя IP-адрес легитимного хоста. Таким образом, пакеты, отправленные из системы мошенников, выглядят так, словно они отправлены с доверенного устройства. Чаще всего IP-спуфинг проводится в рамках масштабной DDoS-атаки, которая может привести к отказу целой сети;

- DNS-спуфинг. Отравление кеша DNS – атакой, во время которой злоумышленник изменяет DNS-записи, чтобы перенаправить пользователя на поддельный веб-сайт, который очень похож на настоящий. Для этого мошенники заменяют IP-адреса DNS-сервера;

- GPS-спуфинг. На GPS-приемник передаются неверные GPS-сигналы, замаскированные под обычные. Мошенники используют такой способ для взлома автомобильной навигационной системы, чтобы направить водителя по неверному адресу, а в более крупных масштабах – для взлома навигационной системы кораблей и самолетов;

- Спуфинг с подменой лица. Злоумышленник может получить биометрические данные пользователя, а затем воспользоваться ими в преступных целях.

Примеры спуфинга.

Используется ложная информация о входящем вызове на вашем смартфоне. Например, звонят якобы с номера 900 или от имени вашего друга.

Аферисты создают вредоносные поддельные сайты с похожими адресами и оформлением. Также аферисты могут установить вирус на устройство под видом рассылки рабочего документа или архива.

Еще одним распространенным примером спуфинга является открытка, отправленная «родственником», и подарок от «маркетплейса».

«Вам открытка» – кто-то из родственников прислал «открытку». Или кто-то из супермаркетов, маркетплейсов присылает картинку – «Вам подарок, выбирайте».

Ни в коем случае нельзя открывать подобные ссылки.

Как не стать жертвой спуфинга.

Не переходите по ссылкам и не открывайте вложения, которые пришли от незнакомого отправителя.

Не отвечайте на письма от неизвестных отправителей и звонки с незнакомых номеров. После общения с мошенниками количество спама может увеличиться.

Обращайте внимание на орфографические и грамматические ошибки на сайтах, в электронных письмах и текстовых сообщениях, а также на другие нетипичные особенности оформления – искаженные логотипы, цвета или неполную информацию. Это может быть признаком спуфинга. Пользуйтесь только теми сайтами, у которых есть действующий сертификат безопасности.

Используйте надежные пароли. Регулярно меняйте пароли и не используйте один и тот же пароль для нескольких учетных записей.

Задействуйте двухфакторную аутентификацию. Это дополнительный уровень защиты ваших устройств и учетных записей.

Не разглашайте личную информацию в Сети.

Регулярно обновляйте устройства и программы. Обновления программного обеспечения обычно включают исправления безопасности, устранение ошибок и новые функции.

Будьте внимательны и не поддавайтесь на уловки мошенников!

Прокурор района

Н.А. Мунатов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 0084AC9267FAF453FE2D456819B4BF50E4
Владелец Мунатов Никита Андреевич
Действителен с 16.04.2024 по 10.07.2025