Виды «обмана» в сети Интернет: вишинг, фишинг и смишинг. Их сущность и принципиальные отличия. Советы, как обезопасить себя от указанных видов мошенничеств.

В настоящее время Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. Общение, покупки, оплаты счетов и различные развлечения постепенно переходят в сеть Интернет.Но, к сожалению, не все используют интернет во благо обществу. Бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений. Появилось множество видов мошенничеств, направленных на получение конфиденциальных данных и дальнейшее их использование в корыстных целях.

К числу самых популярных видов «обмана» в сети Интернет можно отнести фишинг, вишинг и смишинг.

Вишинг, фишинг, и смишинг – это мошеннические схемы, в которых для кражи личных данных с целью дальнейшего взлома банковского аккаунта и незаконного списания средств используются интернет-технологии.

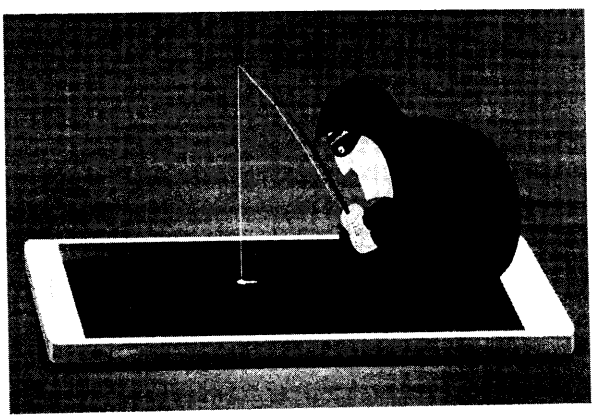
В чем разница между такими похожими, но все же разными видами интернет-мошенничества?

Основная цель у всех одна — выудить конфиденциальную информацию, в основном через перенаправление пользователей на поддельные сайты, но делается это по-разному.

Вишинг *(англ. vishing, от voice phishing) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т.д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом/платежной картой.*

Злоумышленники, представляясь представителями банковских учреждений, силовых структур или иных финансовых учреждений с использованием популярных мессенджеров, таких как Viber и WhatsApp осуществляют звонки на мобильные телефоны граждан и под видом представителя банковского учреждения Республики Беларусь пытаются завладеть реквизитами их банковских платежных карт и иными конфиденциальными данными. Для правдоподобности в качестве имени пользователя (никнейма) они указывают официальный номер банка либо его название, в качестве «аватарки» используют логотип или эмблему банковского учреждения. В процессе общения указанные лица сообщают, что необходимо срочно осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Чтобы предотвратить списание ваших денег, вам предлагается провести нехитрые действия: сообщить 16-значный номер карты и cvv. Также вам может быть предложено установить на ваше устройство – чаще всего на смартфон – специальную «утилиту», которая обеспечит безопасность, а на самом деле – программу для удаленного доступа к Вашему компьютерному оборудованию и мобильным устройствам. Мошенники будут торопить вас и не давать опомниться. Но что действительно повергнет вас в шок, это то, с какой скоростью они спишут у вас деньги, если вы поведетесь на их уловки. В вишинговой схеме может использоваться как робот-автоответчик, так и более «эксклюзивный» вариант с настоящим оператором. Схемы первого типа уже изжили себя, поэтому ставка все чаще делается на живое общение.

Важно! Сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен.



Фишинг *(англ. phishing, от fishing — рыбная ловля, выуживание) — это некий вид получения злоумышленником секретной информации, при котором правонарушитель, используя средства социальной инженерии, «разводит» клиента на открытие своих личных данных. Такими данными могут быть номер и код*

банковской карты, номер телефона, логин и пароль от какого-либо сервиса и т.д.

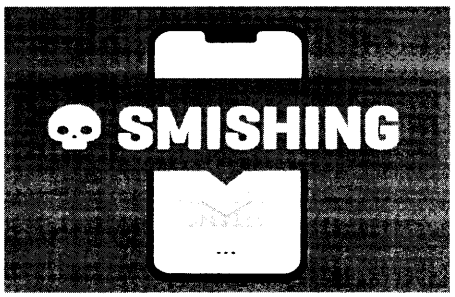
В основном, такой вид «ловли» используют чтобы получить доступ к онлайн-банкингу или кошельку жертвы в той или иной платежной системе и вывести средства на посторонние счета. В качестве своеобразной «удочки» преступники используют специально созданный интернет-сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве «наживки» – некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.

Наиболее часто для совершения такого вида киберпреступлений в Беларуси используется интернет-площадка «Kufar». Сущность схем обмана заключается в следующем: *мошенник* отслеживает на интернет-сайте kufar.by или иной торговой площадке размещенные объявления о продаже чего-либо. Просмотрев абонентский номер автора объявления, находит его в одном из мессенджеров *(Viber, Telegram, WhatsApp)* и вступает в переписку, якобы желая купить выставленный на продажу предмет. Затем пересылает в мессенджере ссылку на поддельную страницу предоплаты, где продавцу нужно ввести реквизиты своей карты для того, чтобы получить деньги от покупателя. При переходе по гиперссылке невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов *(Куфар, ЕРИП, Белпочта, и др.)*. Адрес поддельной веб-страницы также может напоминать реальный *(kufar-dostavka.by, erip-online.com, belarusbank24.xyz и др.)*. Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику. Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

В последнее время участились случаи создания фишинговых сайтов, ориентированных под запросы пользователей в различных поисковых системах. Граждане попадают на них прямо из Google и Яндекса после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска, но не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения,

потерпевший заполняет открывшуюся форму авторизации, данные которой отправляются не банку, а преступнику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.



Смишинг *(англ. smishing – sms+phishing). Данная преступная схема направлена на переход пользователем по вредоносной ссылке из SMS-сообщения. Смишинг представляет собой разновидность фишинговой атаки, для которой основным инструментом становятся смс оповещения.*

Смишинг-сообщение может иметь вид сообщения от известного банка, знакомой компании или быть просто оповещением о внезапном выигрыше в лотерею или в крупную акцию. Сообщение может выглядеть примерно так: «Подписка на платный сервис «Курсы валют онлайн» прошла успешно. С вас будет взиматься 5,99 BYN ежемесячно. Для отказа от сервиса пройдите по ссылке». При переходе по ссылке пользователь попадает на фишинговый сайт, где ему предлагается загрузить вредоностную программу или ввести данные банковской карты.

В случае с SMS выявить подвох несколько сложнее, нежели при фишинге, т.к. сообщения небольшие и имеют меньше информации, помимо самой ссылки.

Как обезопасить себя от фишинга, вишинга, смишинга и других мошеннических схем.

1. Ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Запомните, банк никогда не станет звонить своим клиентам посредством интернет-мессенджеров! Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме.

2. Уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит

указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего, собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;

3. Для того, чтобы проверить законность или правдивость того или иного сообщения от имени банка, свяжитесь с ним по официальному номеру телефона, который указан на сайте банка, в договоре или на вашей карте.

4. Никогда не отвечайте на подозрительные электронные письма или текстовые сообщения, особенно исходящие от людей или компаний, с которыми у вас нет и не было договорных отношений.

5. Обращайте внимание на URL. Мошенники не могут точно имитировать URL-адрес сайта банка или другой компании: он будет отличаться на одну букву или содержать в своем названии какой-то дополнительный символ.

6. Ведите учет сервисов с платными подписками, которыми вы пользуетесь. Если вы получили смишинговое-сообщение от сервиса, на который, как вы думаете, не подписались – скорее всего, никакой подписки не существует. Необходимо помнить, что любые подобные оповещения должны настораживать. Не стоит отвечать на них, следует еще раз перепроверить информацию с помощью звонка на горячую линию подлинного сервиса.

Важно! Если же реквизиты Вашей банковской карты были скомпрометированы, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.