



ФИШИНГ



Обход фильтров
вид фишинга, который использует изображение вместо текста, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами

Социальная инженерия

вид фишинга, который своими действиями заставляет встревожиться пользователя и вызвать у него немедленную реакцию

Неправомерная деятельность, направленная на преступное присвоение доступа к конфиденциальным данным пользователей, таким, как логины, пароли, данные пластиковых банковских карт и др.

Смишинг (SMS фишинг)

вид фишинга, который направлен на рассылку сообщений, содержащих ссылку на фишинговый сайт

Веб-ссылки

вид фишинга, который призван замаскировать подделанные ссылки на фишинговые сайты под ссылки настоящих организаций

Веб-сайты

вид фишинга, который использует JavaScript для изменения адресной строки

Вишинг (голосовой фишинг)
вид фишинга, который направлен на создание сообщений на сайтах для пользователей о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами



Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с неизвестных номеров и не заполняйте никакие формы в Интернете.



Всю информацию, поступившую посредством сети, обязательно проверяйте.



ОСТОРОЖНО МОШЕННИКИ!



Фишинговые атаки

Внимание!

Фишинг – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.



Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с неизвестных номеров и не заполняйте никакие формы в Интернете.



Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги



ПОМНИТЕ вы можете снизить угрозу фишинга, немного изменив свое поведение



САХАЛИНСКАЯ ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

интернет-мошенники!

Хищение денег у пользователей под видом продажи товара ненадлежащего качества, не соответствующего заявленному с использованием интернет-площадок

Продажа несуществующей в реальности продукции в лже-интернет-магазинах

Для кражи личных данных мошенники создают специальные фишинговые сайты, сайты «двойники»

В фишинговом письме может содержаться вредоносный вирус

Хищение денег с банковских счетов при использовании неправомерного доступа к банковским картам потерпевшим



Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети

Не производите предоплату товара. Деньги можно отдавать только в том случае, если заказанный товар проверен и полностью устраивает

При осуществлении входа на сайты уже известных Вам банков или организаций внимательно изучите открывшуюся страницу: она может оказаться сайтом двойником

Ни под каким предлогом, и ни при каких обстоятельствах не сообщайте незнакомым людям цифры, написанные на Вашей банковской карте

Игнорируйте звонки и sms с незнакомых номеров и не заполняйте никакие формы в Интернете

Всю информацию, поступившую посредством сети, обязательно проверяйте!