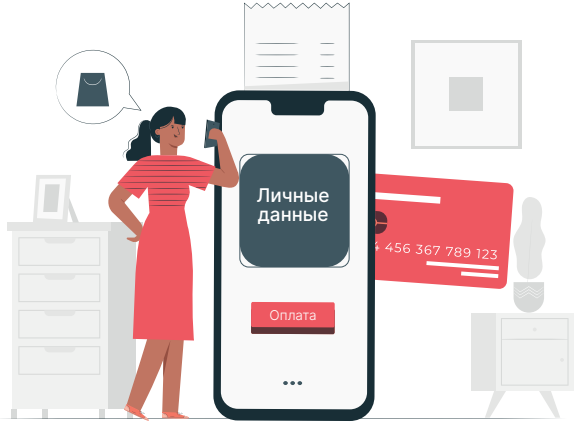
- Используйте инструменты браузера: «избранное», «закладки», «быстрый доступ»;
- проверяйте адрес сайта;
- обратите внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке);
- игнорируйте звонки и смс с незнакомых номеров и не заполняйте никакие формы в интернете;
- внимательно проверяйте внешний облик сайта;
- пользуйтесь только защищенными сайтами: https (где «s» означает «secure» – безопасное);
- не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.



БУДЬТЕ ВНИМАТЕЛЬНЫ!

Всю информацию, поступившую посредством сети, обязательно проверяйте.

Приобретая и размещая товары и услуги через сайты бесплатных объявлений,

ПОМНИТЕ!

- Не вносите какие-либо предоплаты за товар, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наём;
- оплачивайте товар по возможности при личной встрече и после проверки;
- никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код, номер карты и дату окончания срока действия).

ОБРАЩАЙТЕ ВНИМАНИЕ, ЕСЛИ:

- потенциальный покупатель звонит вам из другого региона;
- покупатель соглашается купить товар не глядя;
- покупатель не соглашается на другие варианты оплаты, кроме электронных платежей;
- покупатель не готов встречаться лично, не говорит адрес доставки товара и прочие данные;
- не верьте, если продавец предлагает вам копии своих документов (паспорт, водительские права, ИНН) в качестве подтверждения его личности.

Напечатано по заказу министерства финансов Сахалинской области в рамках региональной программы «Повышение финансовой грамотности в Сахалинской области на 2021–2023 годы»

УМВД России
по Сахалинской области

ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!
интернет-мошенники

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к вашим логинам и паролям.

Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Кражи зачастую происходят через рассылки электронных писем от имени популярных брендов, а также личных сообщений, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.

Фишинг основан на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: **сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее.**

Чем опасны сайты-подделки?

- крадут пароли;
- распространяют вредоносные ПО;
- навязывают платные услуги.

К основным методикам и техникам фишинга относят:

ПРИЁМЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

(Фишеры чаще всего называют себя представителями известных компаний и сообщают покупателям, что им нужно по каким-либо причинам срочно передать или обновить персональные данные. Такое требование мотивируется утерей данных, поломкой в системе или другими причинами. Человек всегда реагирует на значимые для него события. Организаторы фишинга стараются встревожить пользователя и вызвать его немедленную реакцию. Так, считается, что электронное письмо с заголовком «Чтобы восстановить доступ к своему счету...» привлекает внимание и заставляет человека пройти по ссылке для получения более подробной информации.

ФИШИНГ С ОБМАНОМ

Фишер присылает фальшивое письмо от имени организации с просьбой пройти по ссылке и проверить данные учетной записи. А для кражи личных данных создаются специальные фишинговые сайты, которые размещаются на домене максимально похожем на домен реального сайта. Фишинговый сайт оформляется в похожем дизайне и не вызывает подозрений у попавшего на него пользователя.

РАССЫЛКА ВИРУСОВ

Ссылка из фишингового письма может содержать вредоносный вирус.

ФАРМИНГ

Новая разновидность фишинга. Фишеры получают личные данные не через письмо и переход по ссылке, а непосредственно на официальном сайте. Они меняют цифровой адрес официального сайта на DNS-сервере на адрес подменного сайта и, в результате, ничего не подозревающий пользователь перенаправляется на поддельный сайт. Такой фишинг самый опасный, поскольку подмену увидеть нельзя.

Как уберечь себя от фишинга?

- переходя на сайт банка проверять наличие защищенного входа (зеленая полоса перед строкой ссылки);
- никому не сообщать пароли от банковских карт (ПИН-код и пароль интернет-банка);
- не отправлять информацию с вашей карты третьим лицам;
- звонить только на проверенные номера банка;
- смотреть номер отправителя и телефон, который указан для связи, а не верить смс.

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди смогут снизить угрозу фишинга, немного изменив свое поведение. Так, в ответ на письмо с просьбой «подтверждения» учетной записи специалисты советуют **связаться с компанией, от имени которой отправлено сообщение**, для проверки его подлинности. Кроме того, эксперты рекомендуют **самостоятельно вводить веб адрес организации в адресную строку браузера вместо использования любых гиперссылок** в подозрительном сообщении.