Качесовой С.Н
отправить
во все ОУ
Тымк

УМВД России по Сахалинской области

ОТДЕЛ
МИНИСТЕРСТВА ВНУТРЕННИХ
ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ТЫМОВСКОМУ ГОРОДСКОМУ
ОКРУГУ
(ОМВД России по Тымовскому
городскому округу

ул.Первомайская,3, п. Тымовское, 694400
тлф. (4242)780-855; факс (42447)22-5-32

03.06.2021 40/4315

Руководителю управления
образования муниципального
образования «Тымовский городской
округ»

Н.С. Борисенко

694400, Сахалинская область,
Тымовский район, пгт. Тымовское,
ул. Парковая, 9

Уважаемая Наталья Сергеевна!

В связи с участившимися случаями мошенничеств при помощи информационно-телекоммуникационных технологий прошу Вас довести по подчиненных информацию о профилактике указанных выше преступлений, так же прошу распространять памятки посетителям, при возможности разместить наглядный материал (памятки) на информационных стендах Управления образования муниципального образования «Тымовский городской округ».

В случае необходимости в получении памяток в электронном виде обращаться по телефону 89140855638, либо на электронный адрес: ssidelev2@mvd.ru.

Заместитель начальника полиции
майор полиции С.А. Сиделёв

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0243697101CBAC0194419F9AF68F079681
Владелец **Сиделев Сергей Анатольевич**
Действителен с 10.02.2021 по 10.05.2022

К основным методикам и техникам фишинга относят:

- приемы социальной инженерии.

(фишеры чаще всего представляются 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.

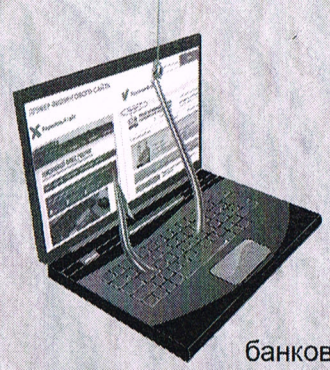
Фишер присылает фальшивое письмо от имени организации с просьбой пройти по ссылке и проверить данные учетной записи. А для кражи личных данных создаются специальные фишинговые сайты, которые размещаются на домене максимально похожем на домен реального сайта.Фишинговый сайт оформляется в похожем дизайне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

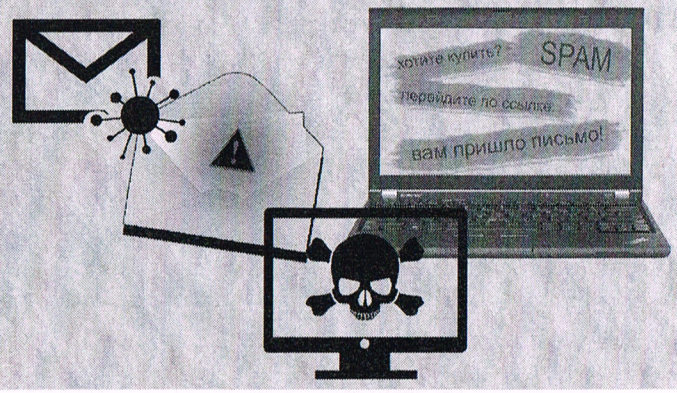


Фишинг – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени 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, являющееся 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



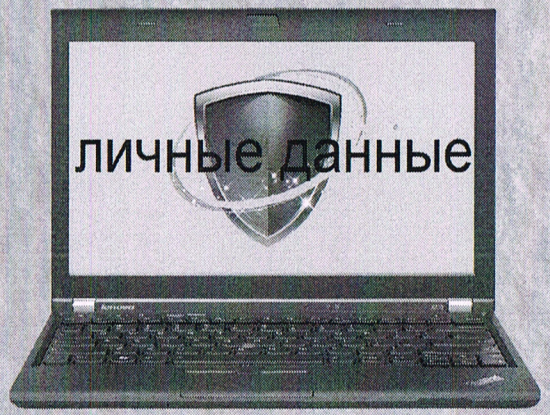
УМВД России по Сахалинской области

ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО

интернет-мошенники!

*Используйте инструменты браузера: «избранное», «закладки», «быстрый доступ»;
*Проверяйте адрес сайта;
*Обратите внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во в сплывающейся 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.

Как уберечь себя от фишинга?

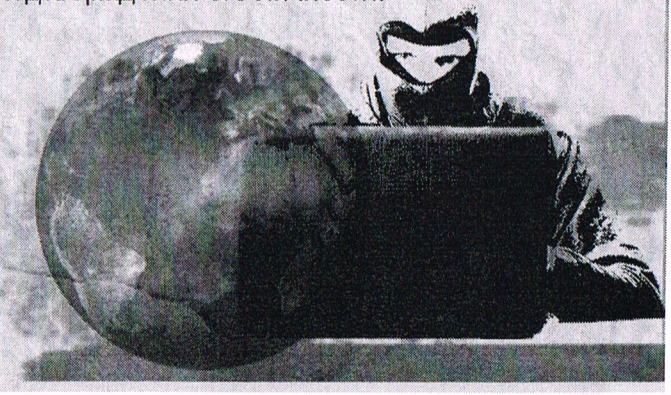
-переходя на сайт банка проверять наличие защищенного входа (зеленая полоса перед строкой ссылки);
-никому не сообщать пароли от банковских карт (ПИН-код и пароль интернет-банка);
- не отправлять информацию с вашей карты третьим лицам;
- звонить только на проверенные номера банка;
- смотреть номер отправителя 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 (или другой обычной просьбой фишеров) 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.

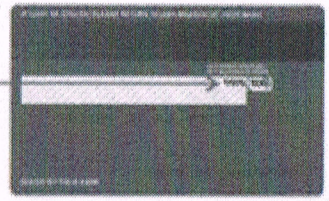
Приобретая и размещая товары и услуги через сайты бесплатных объявлений,

помните!

- 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;
Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/C VV2 код, номер карты и дату окончания срока действия);
Обращайте внимание, если:
- потенциальный покупатель звонит Вам из другого региона;
- Человек 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.



СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?	ЧТО ДЕЛАТЬ?	
ТЕЛЕФОН: Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали	ПРЕРВИТЕ РАЗГОВОР, НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА	ПОЗВОНИТЕ В БАНК
	НИКОМУ НЕ СООБЩАЙТЕ СЕКРЕТНЫЙ КОД	
ТЕЛЕФОН: Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы	ПРЕРВИТЕ РАЗГОВОР, ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ	
ИНТЕРНЕТ: Вы покупаете товар на интернет-площадке (сайте)	ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ ПОЛУЧЕНИИ ЗАКАЗА, ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО НА ПРОВЕРЕННЫХ САЙТАХ	
ИНТЕРНЕТ: Вы продаете товар на интернет-сайтах	НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ И НОМЕРА ПРИХОДЯЩИХ СМС-СООБЩЕНИЙ	
ДОМ: К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара	НЕ ОТКРЫВАЙТЕ ДВЕРЬ	
	НАБЕРИТЕ НОМЕР БЛИЗКОГО ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ	102