Меры безопасности и профилактика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Презентация подготовлена

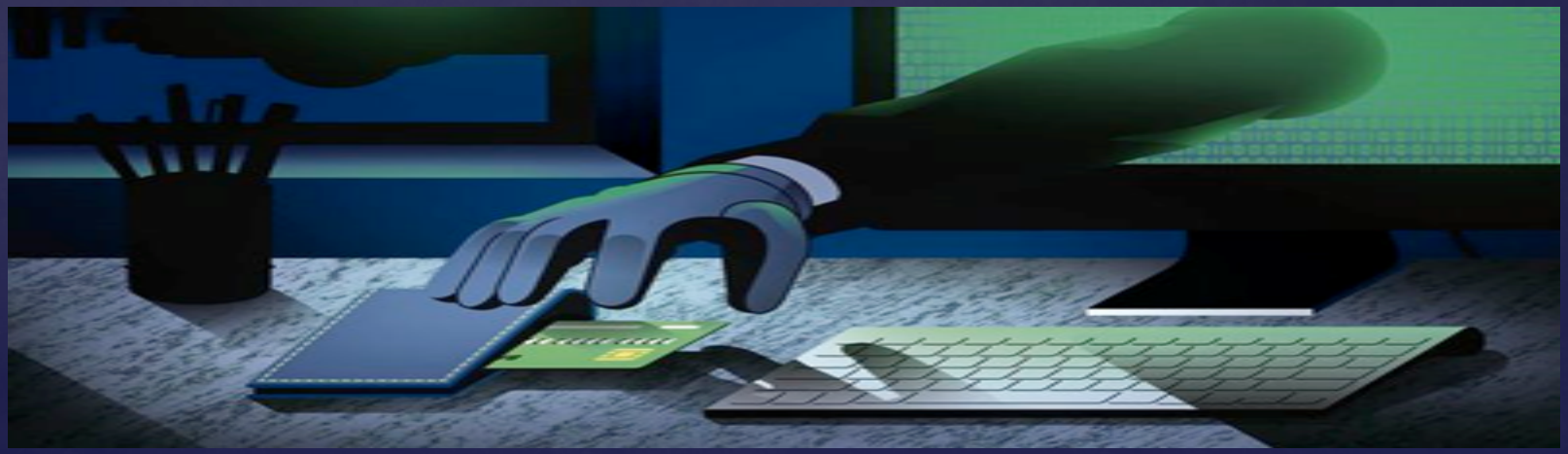
Департаментом информационных технологий Орловской области

с использованием материалов, предоставленных:

- Управлением Министерства внутренних дел Российской Федерации по Орловской области
- Отделением по Орловской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу,
- Управлением Федеральной службы по надзору в сфере связи,
- информационно-аналитическим управлением Администрации Губернатора и Правительства Орловской области.

Преступления в сфере информационных технологий включают:

- распространение вредоносных программ, взлом паролей,
- кражу номеров банковских карт и других банковских реквизитов,
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет,
- вредоносное вмешательство через компьютерные сети в работу различных систем.



Какие схемы используют аферисты?

ОБЕЩАЮТ «ЗОЛОТЫЕ ГОРЫ»

Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты, предложения работы фрилансера за предварительную оплату обучения.

СОВЕТ: Гарантия быстрого обогащения – признак обмана! Игнорируйте заманчивые предложения! Изучите их более детально, прежде чем вкладывать реальные деньги.

ЗАМАНИВАЮТ НА «РАСПРОДАЖИ»

Регулярно размещают товары на сайте объявлений по очень выгодной цене, которая может быть на 30-40% ниже среднерыночной. Единственным условием покупки является внесение небольшого аванса на карту. После получения предоплаты исчезает не только «продавец», но и объявление с сайта. Очень часто наивные пользователи заказывают товар, внося предоплату и в итоге не получают ни посылки, ни денег.

СОВЕТ: Проверяйте юридический адрес магазина, лицензии и ищите отзывы реальных покупателей. Если вы на 100% не уверены в честности продавца, то придерживайтесь покупок исключительно наложенным платежом.

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы, предлагают получить государственные дотации.

СОВЕТ: Не поддавайтесь эмоциям! Не сообщайте свои персональные данные.

МАСКИРУЮТСЯ

!! Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений, крадут у человека персональные данные или деньги с помощью сайтов-подделок (фишинг).

!! Присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки искусного мошенника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки.

СОВЕТ:

- Не доверяйте незнакомцам, не отвечайте на звонки с незнакомых номеров, тщательно проверяйте документы у сотрудников государственных органов.
- Помните, на большинстве фриланс-бирж начать работу можно абсолютно бесплатно.

ИСПОЛЬЗУЮТ ВАШИ ГАДЖЕТЫ

!! По всему миру активно распространяются вирусы-вымогатели, которые попадают на компьютер «жертвы» и зашифровывают все файлы, что ставит под угрозу всю хранившуюся информацию и парализует работу. Чтобы вернуть все ваши документы, вирус выдает сообщение с требованием перевести средства на криптовалютный кошелек, чтобы их невозможно было отследить. Только якобы после этого вы сможете возобновить доступ к файлам. К сожалению, в большинстве случаев вся информация так и остается зашифрованной даже после уплаты «выкупа».

!! Одним из вариантов хищения ваших личных данных является установка зловредных приложений под видом обычных программ.

СОВЕТ:

- Установите антивирус и регулярно обновляйте его.
- Никогда не загружайте приложения на телефон из других источников, кроме официальных магазинов приложений RuStore, RuMarket, NashStore.

ВНЕДРЯЮТСЯ В СОЦСЕТИ

!! Еще один способ выудить информацию у доверчивых пользователей - создание поддельных личных страничек с целью знакомства и получения личной информации, которая может послужить доступом к вашим реальным финансам.

!! Звонки и даже видео-звонки в интернет-мессенджерах от сотрудников банков, работников полиции, прокуратуры с целью выведать у человека его персональные данные.

СОВЕТ: Никогда не раскрывайте свои персональные данные в диалоге с незнакомым человеком или при прохождении сомнительного опроса в соцсети.

ЗАТРАГИВАЮТ СОЦИАЛЬНО УЯЗВИМЫЕ СЛОИ НАСЕЛЕНИЯ

!! В поле зрения мошенников попадают пожилые люди, испытывающие сложности при освоении современной техники, а также страдающие излишней доверчивостью.

!! Многие дети и даже люди старшего поколения обожают игры. Желание быть лучшим порождает зависимость, которая проявляется в растрате денег на своих игровых персонажей для покупки виртуальных улучшений и предметов. Чтобы сэкономить, многие ищут, где это можно сделать подешевле, наталкиваясь на аферистов, которые берут предоплату, но не предоставляют виртуальные ценности.

!! Под прицелом мошенников – крепкие родственные связи. Преступники зачастую представляются близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации.

СОВЕТ: Следите за собственными детьми, если они играют в сети.
Помогите пожилым родителям разобраться в мерах противодействия мошенникам.

Признаки интернет-мошенника!

- На вас выходят сами. Аферисты могут представиться службой банка, налоговой, прокуратурой, полицией. Любой неожиданный звонок, СМС или письмо – повод насторожиться.

- Говорят о деньгах. Предлагают спасти сбережения, получить компенсацию или вложится в инвестиционный проект.

- Просят сообщить данные. Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений.

- На вас давят. Аферисты всегда торопят, чтобы у вас не было времени все обдумать.

- Радуют внезапной выгодой или пугают. Сильные эмоции притупляют бдительность.

Уголовная ответственность за мошенничество в Интернете

Такие преступления караются согласно ст. 159 и 159.6 УК РФ, причём последний пункт подразумевает именно деяния, при которых хищение средств осуществлено посредством информационных систем. Максимальное наказание, предусмотренное по этой статье, составляет 10 лет лишения свободы со штрафом в сумме до 1 млн. рублей.

В наш век развития информационных технологий интернет является точно таким же местом совершение преступления, как и любое другое. Ответственность за любые мошеннические действия предусмотрена статьёй 159 УК РФ, и именно согласно ей составляется заявление на мошенников в интернете от потерпевшего. Она содержит в себе разные пункты в зависимости от суммы причинённого ущерба и способа проведения аферы.

Если мошенников поймали быстро, и сумма причинённого ущерба составляет менее 2.500 рублей, то возможно применение к ним не уголовной, а административной ответственности. При этом наказание варьируется от штрафа до ареста на 15 суток.

Как избежать мошенников в Интернете:

общие правила безопасности.

- **Установите антивирус** и регулярно обновляйте его.
- **Обновляйте приложения**. Этот процесс купирует уязвимые места в программах, которыми могут воспользоваться мошенники для своих действий.

- **Не оставляйте свои персональные данные** на общедоступных ресурсах. Их собирают роботы аферистов, чтобы при контакте с вами вызывать больше доверия и повысить вероятность обмана.

- **Минимизируйте контакты со случайными сайтами**. Высока вероятность того, что, загружая что-либо с неизвестного сайта, вы получите вредоносную программу.

- **Проявляйте осторожность с письмами**. Если вы сомневаетесь в надёжности отправителя, то лучше не переходить по ссылкам, указанным в письме, и не открывать предложенные приложения. Вредоносная программа может быть замаскирована даже под обычный документ Word.

- Всегда **проверяйте адреса электронной почты и сайтов** – они могут отличаться от официальных лишь парой символов.

- **Не пытайтесь «отписаться» от спама, если в письме есть на это ссылка**. Возможно, кликнув по соответствующему баннеру, вы перейдёте на вредоносный сайт. Кроме того, ответная реакция на письмо покажет мошеннику, что ваша почта реально существует и её читают, что простимулирует афериста к применению по отношению к вам более убедительных способов воздействия.

- **Не переходите по ссылкам от незнакомцев** – сразу удаляйте сомнительные сообщения.

- **Никому не сообщайте свои персональные данные**.

- Никогда **не загружайте приложения на телефон из других источников**, кроме официальных магазинов приложений RuStore, RuMarket, NashStore.

- Заведите **отдельную дебетовую карту для платежей** в Интернете и кладите на нее определенную сумму перед оплатой.

Что делать, если мошенники вас обманули?

ЕСЛИ УКРАЛИ деньги с банковской карты!

1 ЗАБЛОКИРОВАТЬ карту

- По номеру телефона банка на банковской карте или на официальном сайте
- Через мобильное приложение
- Через личный кабинет на официальном сайте банка
- В отделении банка

2 НАПИСАТЬ заявление о несогласии с операцией

Заявление должно быть написано:

- В течение суток после сообщения о списании денег
- На месте в отделении банка

3 ОБРАТИТЬСЯ в полицию

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

В случае ЛЮБЫХ ФАКТОВ и при ПОДОЗРЕНИИ на МОШЕННИЧЕСТВО обращайтесь в ПОЛИЦИЮ

по круглосуточным номерам дежурной части –

«02»,«102»,«112» и телефону доверия УМВД – 41-38-56.

За информацию, которая будет способствовать поимке мошенников, предусмотрено **вознаграждение**.

Нельзя опускать руки и отрешиться от проблемы. Нужно действовать, ведь преступники должны быть наказаны. Кроме того, возможно, вы поможете другим людям, которые стали их жертвами или могли бы ими стать.

МОШЕННИКИ БУДУТ ПОЙМАНЫ

За шесть месяцев текущего года в Орловской области зарегистрировано 815 против 601 в 2022 году (+35,6%) преступлений общеуголовной направленности по ст. 159 УК РФ, совершенных с использованием информационных технологий. Из них раскрыто 62 против 15 в 2022 году (+313,3%).

Подробно о правилах кибергигиены
читайте на сайте fincult.info