Районный материал ЕДИ

Наиболее распространенные схемы интернет-мошенничества, направленные на хищение денежных средств граждан

Вишинг - завладение платежными реквизитами банковских счетов граждан реализуемые на методах социальной инженерии и психологического воздействия на потерпевших с использованием телефонных вызовов.

В данных схемах злоумышленники звонят на абонентские номера операторов мобильной связи потерпевших и от имени сотрудников банков выведывают у последних информацию необходимую для получения доступа к банковскому счету и возможности распоряжаться находящимися на счету денежными средствами.

Фишинг - вид интернет-мошенничества, при котором данные пользователя утекают через фальшивые приложения и сайты. Для фишинга злоумышленники создают копию популярного сайта или приложения и активно её распространяют. Предлоги для перехода по ссылке могут быть самые разные: от уведомлений о посетителях страницы до угроз слива интимных фото. В любом случае не открывайте ссылки и приложения от незнакомых людей. Перед переходом по ссылке проверяйте правильность адреса. Мошенники часто используют в своей работе ошибки. Например, адрес vkontakte.w6.ru не относится к социальной сети «ВКонтакте» и может быть использован для фишинга. Современные браузеры имеют защиту от фишинга и предупреждают пользователя о небезопасности сайта. Кстати, будьте внимательнее — фишинг распространяется и через СМС.

Взлом учётной записи - почти каждому из нас приходили сообщения с просьбами помочь в трудной ситуации. Мошенников отличает то, что они просят помочь исключительно деньгами. В таких случаях злоумышленники пользуются доверием близких и друзей человека, придумывая самые разные истории. Если это ваш близкий друг, позвоните ему и спросите о произошедшем. Если вы общаетесь редко, попросите предоставить факты и номер телефона, по которому вы сможете связаться. Не переводите деньги человеку, пока не пообщаетесь с ним лично. Чтобы обезопасить свой аккаунт от взлома, проверьте пароль. Надёжный пароль состоит из 9 знаков и более, содержит заглавные буквы, цифры и символы. Эти же правила относятся и к почте, на которую зарегистрирован аккаунт.

Хищения с банковских платежных карт - в текущем году участились случаи совершения противоправных действий в социальных сетях (как правило, это социальная сеть «Вконтакте», т.е. она наиболее распространена среди молодежи), когда злоумышленник завладевает логином и паролем от учетных записей пользователей, в последующем, представляясь данными взломанного пользователя, вступает в переписку с его контактами, под различными предлогами пытаясь завладеть реквизитами банковских пластиковых карт, после чего совершает хищения денежных средств с банковских платежных карт лиц предоставивших реквизиты карт.

Благотворительные фонды и частные сборы на лечение - в сборах на лечение и помощи людям нет ничего плохо, но дело кардинально меняется, когда мы говорим о мошенничестве. Мошенники используют самые разные схемы для сбора денег, при этом конечный результат один: деньги поступают на сторонний счёт, а не на лечение или помощь. Перед тем как отправлять деньги фонду или частному лицу, проверьте:

-Детальные отчёты о поступлениях и тратах.

-Информацию о том, на что уйдут средства, а также конечную цифру сборов.

-Информацию о человеке или фонде, который собирает средства.

Если вы не уверены или не можете отыскать нужную информацию, задайте интересующие вопросы напрямую в фонд. Честные организации расскажут вам о себе и своей работе. Мошенники же часто создают эмоциональный шум, не предоставляя подробной информации. Списки фондов, которым можно доверять, есть на сайтах «Подари жизнь» и «Все вместе».

Выигрыш призов или внезапное наследство - вас попросят оплатить доставку подарка или работу юриста, который подготовит бумаги о наследстве. Схема с подарками часто применяется к пользователям, которые участвуют в розыгрышах по репостам. Разыгрывать мошенники могут всё что угодно: от бесплатного маникюра до автомобиля и квартиры в Минске.

Чтобы раскусить мошенника, достаточно попросить доказательства о том, что выиграли именно вы, а не кто-то другой.

Группы «Отдам даром» - в группах «Отдам даром» участники предлагают обменять или просто подарить ненужные вещи. Чтобы получить бесплатную вещь, участник сообщества делает репост интересующей записи. После определённого времени даритель сам выбирает человека из списка поделившихся и договаривается о сделке. Детские игрушки, тумбочки и посуда не вызывают подозрений, но часто можно наткнуться на объявления о дорогой бытовой и цифровой технике. Отличить обман можно по следующим критериям:

1. Закрытые комментарии и отсутствие подписи в объявлениях. В настоящих группах участники общаются и задают интересующие вопросы о товаре. В группах мошенников комментарии закрыты.

2. Вас просят оплатить доставку. «Вещь уже ваша, нужно просто оплатить доставку», — заверяют недобросовестные дарители. В реальной жизни люди не будут заниматься доставкой ненужных им вещей.

3. Передача вещей происходит не напрямую. Администрация настоящих групп в сделке не участвует, но в группах мошенников сделки происходят через гаранта. Гарант — посредник между получателем и дарителем. Он предостерегает вас о мошенничестве, а затем просит оплатить свои услуги и доставку товара. Позже гарант сообщает вам, что продавец оказался недобросовестным, и возвращает вам стоимость доставки, но стоимость своих услуг он не компенсирует.

4. Мошенники используют фотографии из интернета. На всякий случай проверяйте изображения в поиске.

Покупка товаров в Интернет магазинах с предоплатой - для осуществления своей преступной деятельности мошенники используют социальные сети, а также создают для этих целей интернет - магазины. Участие в подобных схемах подразумевает наличие всевозможных рисков и привлекает лиц, имеющих намерения на противоправное завладение денежными средствами граждан.

Сложность установления интернет мошенников в подобных случаях связана с тем, что интернет - ресурсы могут быть зарегистрированы с помощью зарубежных сайтов, предоставляющих услуги анонимизации.

Чтобы не стать жертвой мошенников необходимо проверить через поисковые системы все данные о пользователе, у которого вы

намереваетесь осуществить покупку товара. Сведения, которые необходимо проверить:

1. Ник (логин).
2. Аккаунты в соцсетях (по имени-фамилии).
3. Skype, ICQ (если указан).
4. Номер телефона.
5. Электронная почта.
6. Номер электронного кошелька (Webmoney, ЯД, QIWI), номер платежной карточки.
7. Отзывы.

Основная гарантия того, что вы попали на добросовестного продавца и не будете обмануты — наличие в сети информации о нем. То есть, если вы проверили ник, телефон и прочие контакты, и в поиске нет информации по ним — это либо мошенник, либо новый пользователь. Оба предполагаемых варианта заставляют задуматься, стоит ли доверять данному продавцу. Отдельного внимания стоят отзывы. Скопируйте часть отзыва (10-15 слов), и вставьте его в поисковую строку. Если найдете множество совпадений на разных ресурсах — это мошенник.

Если вы не хотите стать жертвой интернет-мошенников — всегда проверяйте и сравнивайте любую доступную информацию о пользователе, с которым решили сотрудничать.

Информация
подготовлена ОВД
Речицкого райисполкома