ПРОКУРАТУРА ВОЛОГОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ

В Интернете злоумышленники используют те же приемы, что и в жизни: играют на эмоциях: жадности, страхе, неосведомленности лиц о юридических и технических тонкостях с целью запутать человека, чтобы он допустил ошибку. По-другому интернет-мошенничество именуется фишингом. Только цель такого мошенничества – не наличные денежные средства, а данные банковских карт и электронных счетов, с помощью которых похищаются безналичные денежные средства.

Классическим фишингом считается мошенничество с помощью электронных писем, сообщений в мессенджерах и поддельных сайтов, вредоносных программ и приложений.

Наиболее распространенные схемы мошенничеств в сети Интернет, а также действия, направленные на то, чтобы не стать жертвой мошенничества в сети Интернет:

- **ПОКУПКА НА САЙТЕ ОБЪЯВЛЕНИЙ АВИТО И ВЫИГРЫШ В ИНТЕРНЕТЕ:** Злоумышленник старается обманом получить доступ к важной информации: логинам и паролям, данным банковских карт и паспортов, кодам верификации – всему, что может ему помочь получить деньги.

Классическим фишингом считается мошенничество с помощью электронных писем, сообщений в мессенджерах и поддельных сайтов.

Например, продавец «Авито» предлагает оплатить покупку на постороннем сайте, не имеющего никакого отношения к сайту объявлений.

Другой способ - физическое лицо в Интернете выиграло приз на значительную денежную сумму, который можно получить, введя на сайте в приложении или в всплывающем окне на сайте номер банковской карты и код на оборотной стороне карты.

В указанных ситуациях после выполнения обозначенных манипуляций потерпевший лишается денежных средств, находящихся на банковском счете.

- Не переводите денежные средства в качестве предоплаты! Не вводите на посторонних сайтах, приложениях и в всплывающих окнах на сайтах реквизиты своих банковских карт!

- **ПОЗДРАВИТЕЛЬНАЯ ОТКРЫТКА:** На абонентский номер лица посредством СМС-сообщений либо через мессенджеры поступает электронная поздравительная открытка, которая может скрывать за собой фишинговые ссылки либо вредоносное программное обеспечение.

В случае нажатия гражданином на такую картинку в своем телефоне может произойти переход на подозрительную ссылку и последующую установку вредоносного программного обеспечения.

В результате этого злоумышленникам открывается доступ ко всем персональным данным пользователя, логинам и паролям его онлайн-кабинетов, установленным в его сотовом телефоне, в результате чего преступникам не составит труда использовать добытые сведения для совершения хищений денежных средств, находящихся на банковском счете.

При этом злоумышленники могут отправлять такие открытки также со взломанных аккаунтов социальных сетей друзей и близких родственников

- Увидев в своем телефоне праздничную картинку либо иной документ, пересланный посредством мессенджера или СМС-сообщения, ни в коем случае не нажимайте на него и не переходите ни по каким ссылкам.

- **ДОХОД В ИНТЕРНЕТЕ: ФИНАНСОВЫЕ ПИРАМИДЫ, ЛЕГКИЙ ЗАРАБОТОК, СДЕЛКИ С КРИПТОВАЛЮТОЙ:** Злоумышленники в сети Интернет размещают сайты и приложения для регистрации и получения дохода от скачивания программ и приложений и их установки на персональные компьютеры и смартфоны, просмотра рекламы, написания отзывов, выполнения иных простых действий.

Все указанные манипуляции производятся лишь с одной целью: получить сведения о банковских картах и счетах граждан, их паролях для последующего хищения безналичных денежных средств, которые вводят в приложениях, на сайтах и в всплывающих окнах их собственники.

Современные финансовые пирамиды в сети Интернет маскируются под инвестиции в криптовалюту, кэшбэк-сервисы, сетевые магазины, совместные покупки, майнинг, игру в накопление денег.

Лица добровольно перечисляют денежные средства злоумышленникам в надежде

заработать высокие проценты с их временного пользования.

Как показала практика, такие интернет-проекты очень быстро закрываются, а их вкладчики – остаются как без вложенных денежных средств, так и без начисленных на них процентов.

Сделки с криптовалютой, в том числе по цене ниже установленного криптообменниками курса, также преследуют за собой цель обмануть ее потенциального покупателя (приобретателя) в силу его неосведомленности о самой технологии покупки (обмена) криптовалюты, убедив его перевести денежные средства якобы для покупки криптовалюты на посторонний счет.

Криптовалюты анонимны, и их перевод практически невозможно отследить, чем и пользуются злоумышленники, предлагая лицам заработать на этом.

Следует отметить, что бесплатный сыр только в мышеловке, все вышеперечисленные предложения – это обман.

- Не устанавливайте незнакомые приложения и программы на свои персональные компьютеры и смартфоны, не вводите сведения о своих банковских картах на посторонних сайтах и приложениях, не переводите денежные средства с целью «легкого» заработка в сети Интернет.

- **МОШЕННИЧЕСТВО СО ВЗЛОМОМ ЛИЧНОГО КАБИНЕТА НА ПОРТАЛЕ ГОСУСЛУГ:** Злоумышленник звонит пенсионерам и инвалидам, представляясь работником органа социальной защиты, сообщая о том, что скоро пенсия будет выплачиваться в «цифровых рублях». Далее «псевдоработник» предлагает отказаться от «цифрового рубля» путем захода на специальный сайт в сети Интернет, где необходимо заполнить заявление и затем его «подписать» через СМС-сообщением.

После выполнения лицом указанных манипуляций злоумышленники получают доступ к мобильному банку и личному кабинету на портале Госуслуг, в результате чего они могут похитить все находящиеся на банковском счете лица денежные средства, а также оформить иные кредиты от имени потерпевшего.

Следующий способ взлома портала Госуслуг: **«Вам необходимо сделать перерасчет за ЖКУ».**

Поступает звонок якобы от сотрудника управляющей компании или ресурсоснабжающей организации, который сообщает лицу о том, что произошла ошибка путем зачисления на лицевой счет большой суммы за жилищно-коммунальные услуги.

Для осуществления перерасчета ее начисления необходимо подать заявление и «подписать» его через код в поступившем СМС-сообщении, который сообщить инициатору звонка.

После выполнения лицом данных манипуляций злоумышленники получают доступ к его личному кабинету на портале Госуслуг.

- Не вводите на посторонних сайтах свои персональные сведения, абонентские номера и номера банковских карт, никому не сообщайте поступающие Вам на телефон коды. Прекратите телефонный разговор.

Прокуратура Вологодской области

Как не стать жертвой мошенничества в сети Интернет

г. Вологда, 2024