ГКП на ПХВ «Городской онкологический цент»
УЗ г.Шымкент

Протокол № - 04

г.Шымкент 15.09.2024г.

Тема: Борьба с коррупцией
Присутствовали: заместители руководителя: Асабаева Р.И., Жумагали Д.Ж., заведующие отделениями, комплаенс-офицер Алихан Б.Е.,
Выступила комплаенс-офицер Алихан Б.Е.: - Добрый день, у нас сегодня несколько актуальных на данный момент тем, хотелось бы начать с темы «Мошенничество», так же я подготовила раздаточный материал /листовки информационные по теме «Мошенничество в интернете» и «Антитеррор»/, прошу после собрания получить и проинформировать тех сотрудников , кто по каким либо обстоятельствам не смог присутствовать сегодня. Если вдруг Вы стали жертвами таких мошенников, следует незамедлительно обратиться в соответствующие органы по мету совершения преступления. Все материалы по данной теме взяты в доступных, открытых сайтах в интернете.
Самыми распространенными видами мошенничества в интернете являются следующие махинации:
Фишинг – кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. Мошенничества в интернете и его виды:
1. Электронные кошельки.

Сейчас электронные кошельки обретают все большую популярность среди интернет-пользователей. Есть разные виды кошельков. Их можно создать на различных площадках.

Один из вариантов мошенничества основан на рассылке на почту писем с уведомлением о блокировке кошелька. Для решения проблемы пользователю предлагается перейти по ссылке или осуществить ввод личных данных. Этого делать нельзя ни в коем случае. В случае подозрения на возникновение каких-либо проблем с кошельком, лучше всего обращаться непосредственно в службу поддержки той площадки, на базе которой вы создали свой кошелек.
2. СМС мошенники.

Этот тип мошенничества крайне прост. Вам поступает просьба об отправке сообщения на определенный номер. При этом вас уверяют, что это полностью бесплатно или плата чисто символическая. После того, как вы сделаете то, о чем вас просят, с вашего счета списывается либо весь остаток средств, либо сумма, в разы большая по сравнению с заявленной стоимостью смс.

Стоит помнить о том, что ни одна солидная организация такими рассылками заниматься никогда не станет.

Нельзя отправлять никакие сообщения. Если же соблазн велик, то самое лучшее – это позвонить в службу поддержки вашего оператора и уточнить у него лично цену этого сообщения на конкретный номер.

Также это можно сделать, если через любую поисковую систему поискать номер того телефона, на который вас просят отправить сообщение.
3. Блокировка системы Windows.

Персональный компьютер может быть заражен вирусами, если пользователь при пользовании интернетом не активирует систему защиты. Таких вирусов огромное множество. У них разные цели и функции. Одним из типов таких вирусов являются те, что нацелены на блокировку системы Windows.

С помощью вируса, незаметно и иногда даже автоматически проникшего в компьютер пользователя, добавляется определенный код в автозапуск.

Система блокируется после того, как пользователь перезагрузит компьютер. Как правило, на экране появляется уведомление о том, что вам необходимо отправить сообщение на определенный номер, при желании разблокировать компьютер. Параллельно в сообщении могут быть угрозы о том, что в случае вашего отказа все ваши данные будут удалены.

Не стоит бояться этого типа мошенничества. Через любую поисковую систему или на сайте антивирусных программ можно найти коды для того, чтобы разблокировать ваш компьютер.
4. Фишинг.

Данный тип интернет-мошенничества нацелен на сбор данных персонального характера. С английского языка это слово переводится «выуживание/ловля».

Схема работы фишинга следующая. Вы получаете на почту письмо, уведомляющее вас о срочной необходимости передачи ваших личных данных куда-либо.

Это может касаться, к примеру, вашей банковской карты. При этом часто в виде объяснения причин указывается системный сбой, в ходе которого ваши данные были потеряны или повреждены. Попутно вам могут угрожать блокировкой вашего счета, аккаунта и т. д.

5. Программы, взламывающие разные платежные системы.

Мошенники часто предлагают купить у них чудесные программы, предназначенные для взлома электронных кошельков. После покупки, как правило, обнаруживается, что купленная программа не работает, а в худшем случае даже заражает вирусом ваш компьютер.

6. Взлом аккаунта.

На сегодняшний день многие пользователи имеют свои странички в социальных сетях.

Это породило новый тип мошенничества. В один прекрасный день вы не можете зайти на свою страницу. Вас просят для этого отправить сообщение на конкретный номер.

Это нельзя делать! Это сообщение будет стоить вам немалых денег. Чаще всего проблемы можно решить путем запроса в службу поддержки сети. Оттуда вам вышлют сообщение с новым паролем, введя который вы сможете спокойно продолжать пользоваться своей страницей. Такое сообщение бесплатно! Вообще, в случае любого сомнения в такой ситуации самое лучшее – это обратиться в службу поддержки вашей сети.

7. Финансовая пирамида.

Вам обещают огромные деньги, если вы внесете свой маленький взнос в каком-либо символическом размере (скажем, 10 долларов). При этом ваш заработок будет основан на том, что вы будете сами привлекать своих друзей и знакомых в этот заработок.

Самый распространенный тип компаний, который практикует такой тип мошенничества, – это разные MLM компании, которые продают никому не нужные товары или услуги неоднозначного качества.

Конечно MLM компания отличается от финансовой пирамиды наличием товара, предназначенного для продажи. Финансовая пирамида по сути продает воздух. Но, тем не менее, чаще всего этот товар ужасного качества, что дает основание считать MLM компанию как финансовой пирамидой. Не платите деньги за вступление в такие организации.

Комплаенс офицер Алихан Б.Е.