Конспект по теме:
«Актуальные способы совершения киберпреступлений»

Электронные сервисы, интернет-банкинг, удаленная работа и учеба, социальные сети, интернет-магазины и маркетплэйсы – все это настолько прочно вошло в нашу повседневность, что иногда трудно поверить, как жили без этого раньше. Чем больше мы погружаемся в мир информационно-коммуникационных технологий, тем уязвимее становимся для интернет-преступников.

Киберпреступность не стоит на месте, а активно идет в ногу со временем, с развитием технологий меняются схемы и способы обмана. Отдельное беспокойство вызывает применение искусственного интеллекта в преступной деятельности. По статистике женщины *(65%)* чаще всего становятся жертвами телефонных мошенников, которые выманивают деньги путем психологических манипуляций *(77,9%)*, купли-продажи товаров и оказания услуг *(65,6%)*, благотворительности *(100%)*. Мужчины *(84,8%)*, как правило, становятся жертвами мошенничества, связанного с использованием сайтов знакомств. Большинство потерперших от интернет-мошенничеств в возрасте от 30 до 49 лет, люди сарше 50 лет более подвержены мошенничествам, связанным с помощью родственникам.

Наиболее распространенным способом интернет-хищения денежных средств является **телефонное мошенничество** в различных модификациях. Аферисты представляются работниками банков, коммунальных служб, водоканала, энергонадзора, служб газа и связи, сотрудниками правоохранительных и государственных органов, даже вашими знакомыми и родственниками. Чтобы похитить деньги мошенники под различными предлогами пытаются завладеть личными данными, включая коды из смс. Часто они действуют в паре. Например, первый под предлогом замены ключей от домофона выманивает числовой код из смс, а второй мошенник, представляясь правоохранителем, угрожает проведением обыска и изъятием денежных средств за передачу того самого кода. Или другой пример. Один мошенник представляется руководителем вашей организации и пугает подозрением в экстремистской деятельности и проведением обыска, а другой от имени правоохранителя предлагает якобы помощь в решении данной проблемы: для этого нужно перевести деньги на «временный счет» или передать их курьеру.

Надо помнить, что никаких временных счетов не бывает и вернуть свои деньги с чужого счета невозможно.

Зарегистрированы случаи, когда подростков под угрозой привлечения к ответственности мошенники заставляли открыть сейф и передать лично курьеру деньги родителей. *Оба следующих случая произошли в октябре этого года в Минском районе. Школьник после общения с незнакомкой в*

мессенджере вынес из дома 70 тысяч долларов. В данном случае собеседница узнала геолокацию его школы по отправленному фото, после чего школьник получил видео, в котором человек в балаклаве с украинским флагом сообщил ему, что взломал аккаунт его онлайн-подруги и теперь владеет всей информацией из их переписки. Сразу на связь с парнем вышел неизвестный, который представился сотрудником милиции и сообщил, что передача геолокации иностранцу влечет уголовную ответственность. Вскоре появился еще один псевдомилиционер, который под предлогом декларирования потребовал показать сколько денег имеется в доме. В течение недели мошенники вымогали у парня информацию и угрожали ему. В результате парень узнал у отца код от сейфа и сфотографировал деньги. На следующий день с ним связался якобы сотрудник КГБ, который потребовал срочно передать деньги курьеру. Мальчик положил все деньги в рюкзак и оставил его в лесу. Все действия он транслировал в прямом эфире. Деньги родители собирали на ремонт дома.

Во втором случае 15-летнюю девушку неизвестный по телефону убедил, что необходимо задекларировать все сбережения родителей. По его указанию она отдала курьеру 55 тысяч долларов. Деньги родители копили ей на квартиру.

Также мошенники используют и другие схемы обмана. Аферист по телефону представляется работником банка или предприятия связи (Белтелеком, А1, МТС) и убеждает обновить мобильное приложение, для чего необходимо скачать и установить на телефон поддельное приложение, направленное ссылкой или файлом (*.apk) в мессенджере. Часто такие фейковые приложения предоставляют удаленный доступ к устройству и мошенник «подсматривает» все, что происходит на экране. Иногда этого бывает достаточно, чтобы похитить деньги. В последнее время появилась еще одна возможность. После установки приложения мошенник просит передать пин-код и поднести банковскую карту к задней крышке телефона (к модулю NFC). Так мошенник получает дубликат вашей банковской карты и тоже может похитить деньги.

Нельзя выполнять никаких действий, связанных с финансами, по указанию незнакомых, кем бы они не представились.

Больше всего людей становятся жертвами киберпреступников при попытке купить товар подешевле в социальных сетях или мессенджерах. Часто в мошеннических аккаунтах «продают» одежду, смартфоны, автомобильные шины, садовые кресла, цветы, рыбу и многое другое, то, что нужно доставлять курьером, а не почтой.

Остерегайтесь подозрительно низких цен и не переводите предоплату за товар или услугу, выбирайте оплату наложенным платежом. Прежде чем согласиться на покупку, проверьте наличие

у продавца сайта в белорусском сегменте интернета и созвонитесь с ним по телефону. Тщательно проверяйте информацию о продавце.

Наряду с указанными крупные хищения мошенники совершают с использованием поддельных инвестиционных или криптоплатформ. Размещая рекламу в Интернете, они могут использовать видео с известными людьми – политиками, спортсменами, даже блогерами, которые озвучены фразами, сгенерированными с помощью искусственного интеллекта. Например, на видео может быть известная телеведущая, которая в репортаже рассказывает о якобы новой возможности заработка, или заместитель министра дает интервью, что многие уже пользуются определенным ресурсом и получают деньги, хотя на самом деле все слова – это всего лишь результат работы нейросетей. С заинтересовавшимися связываются так называемые кураторы или брокеры и убеждают участвовать в инвестировании или программе на том самом ресурсе. Для получения пассивного дохода предлагают вложить деньги в прибыльный проект. Часто жертв побуждают к оформлению кредитов для перевода большей суммы. На самом деле вкладчику просто «рисуют» его прибыль на сайте и никогда не дают возможности вывести его деньги.

Нужно понимать, что легких денег не бывает, а бесплатный сыр в мышеловке. Вернуть деньги, «вложенные» подобным образом, невозможно.

Одним из новых, набирающих обороты, способов является вымогательство за разблокировку Iphone. Вначале аферист в переписке узнает о наличии Iphone у будущей жертвы, а потом под различными предлогами убеждает войти в его ICloud. Предлогами могут быть, например, помощь в восстановлении фотографий, сохранение диплома, возможность пройти уровень в игре или получить для своего героя игровое имущество, оружие или способность. После входа в ICloud мошенника, Iphone жертвы блокируется. Для его разблокировки предлагается заплатить сумму, в зависимости от модели, превышающую 1000 рублей.

Это не все, но самые актуальные и распространенные схемы, и со временем они могут меняться. Чтобы не стать жертвой киберпреступников, необходимо всегда адекватно оценивать свои действия и как бы вас не запугивали, не поддаваться панике и страху. Будьте бдительны и берегите свои деньги!

Главное управление
по противодействию киберпреступности
криминальной милиции
МВД Республики Беларусь