УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«Фишинг, вишинг – как вид интернет-мошенничества.
Примеры из практики»

Гомель

(информация изложена для выступления от первого лица)

За последние десятилетия число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц.

В Гомельской области с 2017 года наблюдался устойчивый рост таких преступлений (2017 г. – 370, 2018 г. – 563, 2019 г. – 1781, 2020 г. – 3394). В 2022 году количество преступлений снизилось, за 2 месяцев текущего года в Гомельской области зарегистрировано 295 киберпреступлений, что в 1,9 раза меньше данного показателя 2021 года (561 преступление). Более 90% из выявленных преступлений составляют хищения имущества путем модификации компьютерной информации (ст. 212 УК Республики Беларусь). Кроме этого, отмечается рост количества преступлений в сфере информационной безопасности (28).

Не теряет свою актуальность **завладение реквизитами банковских карт с помощью фишинговых интернет-страниц, имитирующих популярные площадки объявлений**. Через различные мессенджеры с гражданами, разместившими на площадке объявление о продаже различных товаров, велась переписка. В ходе общения потерпевшим предлагалось перейти по ссылке на фишинговую (поддельную) страницу, внешне схожую со страницей торговой площадки, и ввести реквизиты своей банковской карты для якобы отправки на их счет предоплаты. После ввода данных денег продавец не получал, а с его банковской карты списывались имеющиеся на ней денежные средства.

В марте текущего года 34-летняя женщина на популярной торговой интернет-площадке «Kufar» разместила объявление о продаже товара. Посредством мессенджера «Whats App» с ней связался потенциальный покупатель и сообщил, что хочет его приобрести с помощью доставки, после чего переслал фишинговую ссылку. Перейдя по ней, жительница г. Житковичи заполнила реквизиты своей банковской карты, в том числе и остаток на счете. Вместо пополнения баланса потерпевшая лишилась более 190 рублей.

Зафиксированы и случаи, когда гражданам **предлагается оформить доставку товара почтой**. Схема аналогичная: злоумышленники присылают фишинговую ссылку сайта, схожего с сайтом

РУП «Белпочта», на котором якобы оформлена их «сделка». После указания всех реквизитов банковской карты со счета продавца также списываются деньги.

Также, большое количество уголовных дел **возбуждено по факту хищения денежных средств лжесотрудниками банков**. Злоумышленники звонят потерпевшим на мобильные телефоны, представляются работниками различных банков, и под вымышленными предлогами запрашивают реквизиты банковских платежных карт и паспортные данные. В результате доверительного общения граждане лишаются своих сбережений.

К примеру, Житковичским районным отделом Следственного комитета расследуется уголовное дело о хищении более 139 рублей с карт-счета жительницы г. Житковичи. В марте текущего года женщине в мессенджере Viber позвонила женщина и представилась работником технической поддержки банка. Звонившая сообщила, что на имя потерпевшей в банке оформлен онлайн-кредит, и для того чтобы отменить заявку на кредит, ей необходимо установить на телефон определенную программу, этой программой в последующем оказалась программа удаленного доступа «AnyDesk», с помощью которой злоумышленница смогла перечислить деньги со счета потерпевшей на свою банковскую

В практике следователей зафиксирован **еще один способ совершения противоправных действий в сфере информационных технологий** – злоумышленник после несанкционированного доступа к странице в социальной сети рассылает пользователям, находящимся в разделе «Друзья», сообщение с просьбой об оказании помощи в переводе денежных средств под различными предлогами. После чего входит в доверие и, якобы для перевода им денежных средств, просит сообщить реквизиты банковской платежной карты и коды из поступивших на мобильный телефон смс-сообщений или присылает ссылку на фишинговую (поддельную) страницу, внешне схожую со страницей банка. Пользователь, не догадываясь о преступности намерений, сообщает запрашиваемую информацию или вводит данные, в результате чего злоумышленник получает доступ к карт-счету и совершает хищение имеющихся на нем денежных средств.

Помните, что хищение денежных средств с карт-счетов становится возможным только в случае передачи держателем карты ее реквизитов третьим лицам.

В очередной раз сотрудники органов внутренних дел просят граждан быть бдительными:

при использовании торговой площадки «Kufar» совершайте все действия исключительно на самой платформе объявлений;

не переходите по ссылкам, которые высылают неизвестные собеседники;

не предоставляйте третьим лицам сведения об учетной записи в интернет-банкинге и мобильном банкинге;

никому ни под каким предлогом не передавайте реквизиты своих банковских карт, в том числе CVV-код;

если вам звонят с подобными просьбами, представляясь сотрудниками банка, правоохранительных органов, либо иными государственными организациями, прекратите данный разговор и, при необходимости, перезвоните в клиентскую службу вашего банка (номер указан на банковской карте) для уточнения всех вопросов;

помните, что сотрудник банка никогда не будет получать информацию у клиента о ее полных реквизитах, тем более посредством телефонного звонка;

в случае утери банковской платежной карты обратитесь в банк для ее блокировки;

если все же вы стали жертвой киберпреступников немедленно обратитесь в правоохранительные органы.

Расскажите эти правила Вашим родственникам и знакомым, особенно пожилым людям.

https://vk.com/wall-158272399_31274 – пример «развода» с оплатой посредством Европочты.
https://vk.com/wall-158272399_31268 – пример участия в «спецоперации».