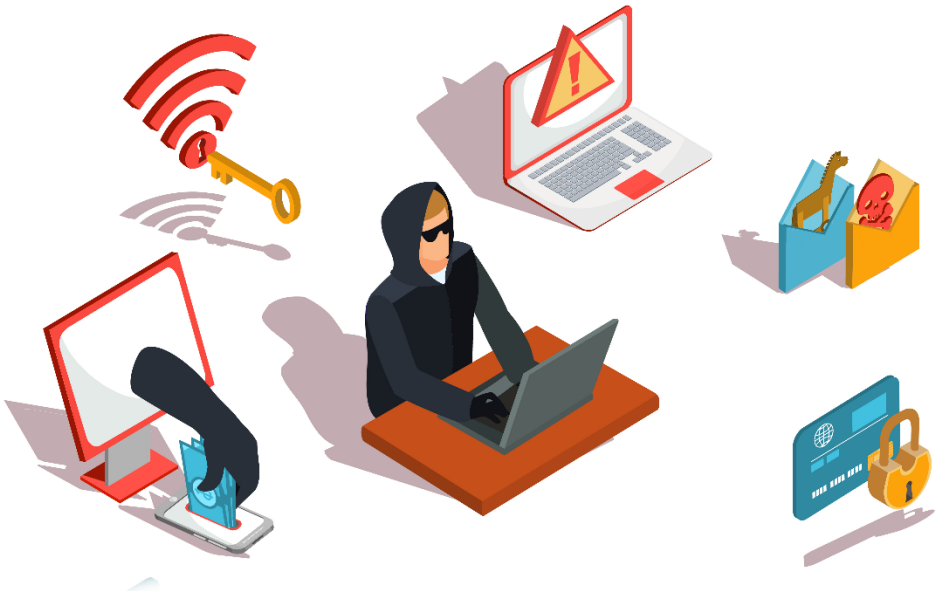
Дневник исследователя.

Истории знакомых, поделившихся в ходе опроса своими случаями, связанными с финансовым мошенничеством. Примеры самых крупных хищений денежных средств через Интернет.

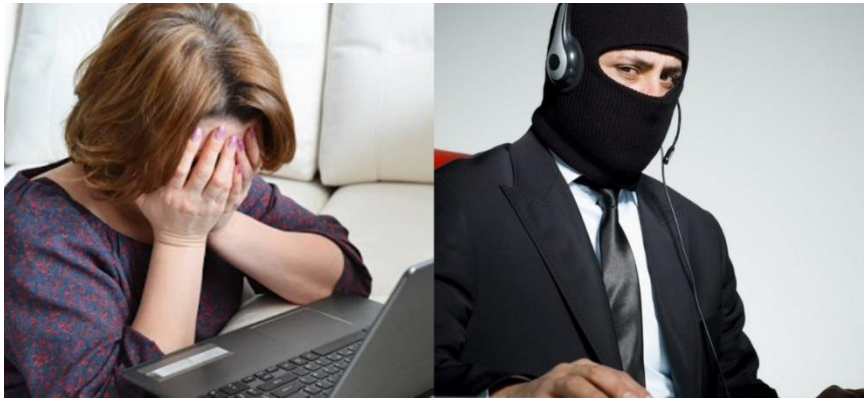


Дневник исследователя.

Первая история. «Ночное спасение близкого»

«Мне мошенники позвонили поздно ночью и сказали, что сын арестован, находится в отделении полиции, при нём были обнаружены наркотические вещества. Злоумышленники предложили «помочь» близкому человеку за 50 тысяч рублей, оказывая при телефонном разговоре постоянное психологическое давление. Главное условие мошенников было следующее: не отключая телефон, совершить перевод денежных средств по указанному ими номеру телефона. Из 50 тысяч первоначально удалось перевести 8 тысяч рублей из-за лимита, установленного Сбербанком на моей банковской карте. Расчет мошенников был сделан на то, что было ночное время, известие очень неприятное, «жизнь разрушилась на глазах»! Но все же, удалось связаться с родственником, убедиться, что он дома и всё в порядке. Я сразу позвонила на горячую линию по номеру телефона, указанному на карте, обратилась в полицию и в банк с письменным заявлением. Через некоторое время со мной связалась служба поддержки, и позже денежные средства в полном объеме были возвращены.»

(Телефонное мошенничество).



Вторая история. «Помощь знакомому»

«Знакомый написал сообщение в социальной сети «Вконтакте» с просьбой занять денежную сумму в 5000 рублей. Не догадалась позвонить и спросить, действительно ли нужна помощь, или задать личный вопрос, чтобы удостовериться в том, что это мой приятель, а не кто-то другой. Подумала, раз человеку срочно нужно, то почему бы не помочь. Перевела по номеру карты. А через пару часов страница знакомого приняла статус «удалено». Оказалось, что приятеля взломали мошенники. Кто вернет деньги, да и как вычислить этих злоумышленников, если они общались со мной через чужую страницу, а потом ее и вовсе удалили. Обращаться я никуда не стала.»

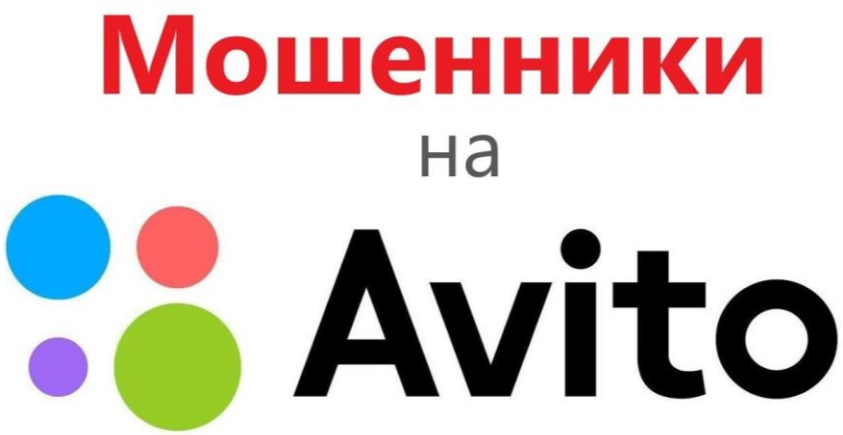
(Кибермошенничество).

Третья история. «Вежливые продавцы»

Один предприниматель разместил объявление о продаже дивана на Авито. Через несколько дней раздался звонок. Девушка с приятным и вежливым голосом сообщила, что она с мужем-военнослужащим сейчас в другом городе, но скоро переезжают в город где живет "жертва". Ей очень понравился диван, и она готова его купить прямо сейчас. И для подтверждения перевода попросила продавца доехать до банкомата, чтобы распечатать какое-то подтверждение.

Предприниматель уже прыгнул в машину, но в последний момент его осенило, что это какой-то обман, т.к. для подтверждения оплаты он может сделать выписку с мобильной версии Сбербанк Онлайн. Он сообщил девушке, что никуда не поедет. Её тон сразу сменился, и она стала довольно настойчиво ему говорить, что он должен именно ехать к банкомату. В итоге разговор перешел рамки дозволенного, и гражданин просто бросил трубку и заблокировал её.

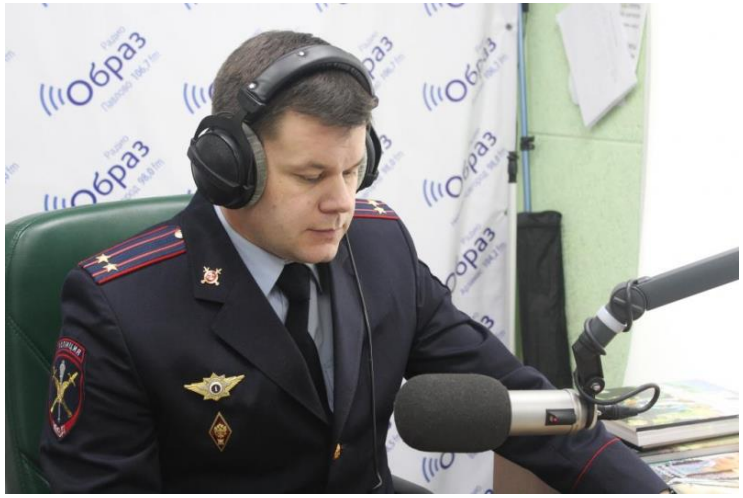
(Кибермошенничество).



Четвертая история. «Приятный сюрприз»

На мобильный телефон абонента звонит лже-ведущий известной музыкальной радиостанции и поздравляет с выигрышем ценного приза. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Дозвонившегося поздравляют, он передает приветы, заказывает песню и узнает еще одну приятную новость: он не просто получит приз – телефон — его сразу же подключат, нужно лишь в течение 30 минут купить карту пополнения счета вышеназванной компании и сообщить ее данные диджею. Заплатив деньги и придя через несколько дней за подарком, обманутый абонент узнает, что на радиостанции никто подобного конкурса не проводил, так что долгожданного телефона он не получит. Да и купленная карточка уже не пригодится — «награждающие» давно перевели с нее деньги на свои счета.

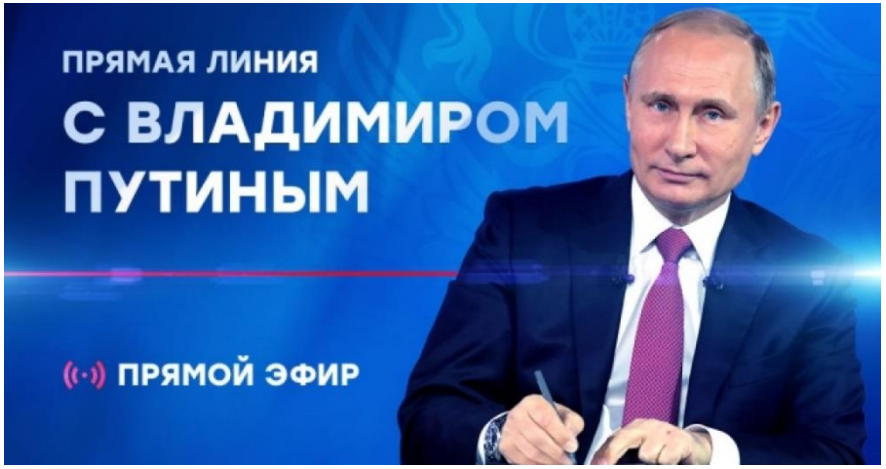
(Телефонное мошенничество).



Пятая история. «Стоимость разговора с президентом»

В Екатеринбурге мошенники пытались заработать на «прямой линии» с президентом РФ. За день до «прямой линии» по сотовому телефону они сообщили жертве, что ее номер выбран компьютером, ее соединят с президентом, но для улучшения качества связи необходимо немедленно на тысячу рублей пополнить счет телефона, с которого поступил звонок. На попытки «избранного» перезвонить по высветившемуся телефону испитой голос один раз представился «прачечной», второй - «залом игровых автоматов», затем абонент и вовсе отключил телефон. В соответствующих органах, которые молодой человек уведомил о странном звонке, его поблагодарили за бдительность.

(Телефонное мошенничество)



Самые известные за всю историю случаи кибермошенничества.

1. Взлом PayPal.

PayPal – система электронных платежей, пришедшая из США и специально созданная для приема платежей через интернет.

В этом преступлении приняли участие челябинские хакеры: Василий Горшков и Алексей Иванов. Они проникали в кооперативные сети PayPal, Western Union, Nara Bank. С помощью обыкновенных домашних компьютеров они украли 16 тысяч номеров кредитных карт и нанесли ущерб на общую сумму 25 миллионов долларов. В 2000 году ФБР удалось поймать взломщиков: друзья получили по три и четыре года тюрьмы.

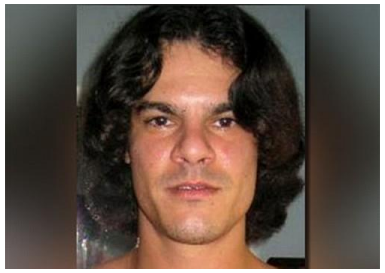
(Василий Горшков и Алексей Иванов)

2. «Фишинг-король»

Валдир Пауло де Алмейда вошел в историю как самый крупный спаймер: на момент его ареста компания «Валдира» рассылала около трех миллионов фишинговых писем в сутки. Вредоносная рассылка занималась распространением «троянов» - вирусов, проникающих в устройство пользователей онлайн-банкинга. По приблизительным подсчетам это позволило «королю спаймеров» обогатиться на 37 миллионов долларов.

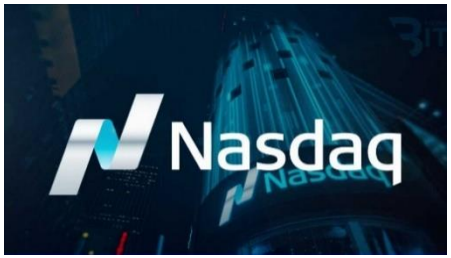
3. Взлом Heartland Payment System

Масштабная атака на банк, подготовленная кубинцем Альберто Гонсалесом. На украденных данных талантливый юноша заработал более 10 миллионов долларов – в основном путем перепродажи информации. Как минимум одну десятую выручки он закопал в саду родительского дома – там ее и обнаружила полиция. Несмотря на раскаяние хакера, суд приговорил его к 20 года тюремного заключения.



(Альберто Гонсалес)

4. Взлом NASDAQ



NASDAQ - американская биржа, специализирующаяся на акциях высокотехнологичных компаний (производство электроники, программного обеспечения и т. п.)

Крупное киберпреступление, организаторами которого выступили российские и украинские хакеры: группа кибермошенников взломала систему безопасности электронной биржи NASDAQ и получила доступ к крупнейшим торговым сетям и банкам Европы и США. Нанесенный ущерб исчисляется сотнями миллионов долларов. Пока пойман лишь один злоумышленник – россиянин Дмитрий Смилянец.

5. Взлом Citibank

Ситибанк - крупнейший международный банк, основанный в 1812 году как City Bank of New York, затем First National City Bank of New York.

Этот кибертеррористический акт организовал россиянин из города Санкт-Петербург – Владимир Левин. Он смог поникнуть во внутреннюю сеть банка и перевести более 10 миллионов долларов на счета в США, Финляндию, Израиль и другие страны. Правда, все переводы, за исключением 400 тысяч долларов, заблокировали, а Левина поймали и приговорили к трем годам лишения свободы.

(Владимир Левин)