Краткий обзор способов совершения киберпреступлений актуальных в настоящее время, используемых при проведении выступлений (информация написана от первого лица).

1) **Вишинг** — это одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка.

Как обычно действуют злоумышленники «вишеры»?

На телефон поступает звонок от сотрудника банка и оператор предупреждает, если прямо сейчас не будет предоставлена полная информация банковской карты ему по телефону, то карту заблокируют. Доверчивый пользователь, слыша подобную «угрозу» сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться столь удачной покупке или выгодной акции, всегда стоит лишний раз перепроверить информацию, обратившись к официальным ресурсам.

В любой непонятной ситуации главное не паниковать. Помните — всегда всё можно проверить. Вежливо попрощайтесь с собеседником и позвоните на горячую линию организации, представителем которой назвался звонивший. Так вы легко сможете понять был ли звонок обоснованным, или вы чуть не стали жертвой вишинга.

Распространенные примеры вишинга:

- Звонки из банка.

Мошенники звонят на мобильные с номеров, которые могут напоминать номер банка. «Здравствуйте, я сотрудник службы безопасности банка», — представляются они. И сообщают, что «банк выявил подозрительную операцию» или «в системе произошел сбой».

Чаще всего «сотрудник службы безопасности» просит сообщить данные карты, CVV- или CVC-код, код из СМС или пароли, поступившие от банка. Или даже перевести все свои деньги на «резервный счет».

Мошенник очень убедителен, звонок поступает якобы с официального номера, а данные просят сообщить не человеку, а роботу.

Также он может озвучить ваши персональные данные, чтобы убедить в необходимости перечисления сбережений на защищенный счет.

Но сотрудник банка никогда не потребует у вас конфиденциальных данных. Например, не попросит назвать номер карты или номер на ее обороте, а также CVC-пароли банка, которые придут вам на телефон в виде

СМС. **Лучше сразу оборвать разговор.** Не совершайте никаких действий, которых требует звонивший, как бы он ни был убедителен.

Очень полезно занести официальные номера вашего банка в записную книжку. Тогда при звонках с похожих номеров у вас будет высвечиваться контакт «Неизвестный номер».

- Установка программ удаленного доступа на устройство.

Злоумышленник звонит пользователю, представляясь сотрудником банка, и сообщает, что зафиксирована попытка взлома его личного кабинета или же вывода средств с его счета. Якобы службе безопасности банка требуется помощь клиента: нужно решить техническую проблему для противодействия мошенничеству. Для этого необходимо срочно установить программу удаленного управления смартфоном (Any Desk или Team Viewer), чтобы сотрудники банка могли получить доступ к устройству и обезопасить пользователя. После установки такой программы, мошенник получает возможность действовать от имени пользователя и, получив доступ к приложению мобильного банкинга, выводит средства со счета жертвы.

- Звонки от лжесотрудников милиции, прокуратуры и т.д.

Усложненный, двухступенчатый сценарий начинается со звонка от фейкового представителя ОВД (следователя, сотрудника КГБ и т.д.). С помощью специальных средств IP-телефонии номер злоумышленника может быть подменен и выглядеть как реальный телефонный номер одного из отделений ОВД. Фальшивый милиционер расскажет вам про участившиеся случаи мошенничества или про утечку данных из известных банков и сообщит о риске для денежного счета клиента – вас. При этом он подчеркнет, что саму беседу вы должны держать в тайне от всех членов семьи и знакомых, так как это «следственная тайна». Для убедительности мошенник даже может напомнить о базовых правилах безопасности, а именно – о том, что никому нельзя называть код из СМС. Предположим, вы поверили и заинтересовались. Что происходит дальше?

Выработав определенный кредит доверия к себе, лжесотрудник милиции скажет, что необходимо провести ряд мер, направленных на противодействие мошенникам, и для этого переведет вас уже на второго человека, «сотрудника банка» или «службы безопасности» (а по факту на такого же преступника, как и он сам). Дальше все развивается по классическому сценарию: жертву просят либо установить на телефон специальное приложение для удаленного доступа, с помощью которого злоумышленники получают доступ к мобильному банку, либо оформить

«защищенный» счет и перевести на него деньги. В случае если вы поведетесь, все закончится для вас пустым счетом и сожалением.

В другом варианте схемы мошенники меняются местами: «милиционер» подключается только после разговора жертвы с классическим «сотрудником безопасности банка». После того как жертва отказывается выполнять предложение оформить кредит онлайн или установить приложение, сказать код из СМС и прочее, звонящий «милиционер» убеждает послушаться своего липового коллегу из службы безопасности банка.

2) **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание) — это некий вид получения злоумышленником секретной информации, при котором правонарушитель, используя средства социальной инженерии, «разводит» клиента на открытие своих личных данных. Такими данными могут быть номер и код банковской карты, номер телефона, логин и пароль от какого-либо сервиса и т.д. В основном, такой вид «ловли» используют чтобы получить доступ к онлайн-банкингу или кошельку жертвы в той или иной платежной системе и вывести средства на посторонние счета.

Так как же работает фишинг?

На электронный адрес атакуемого приходит фишинг-письмо, которое, в первую очередь, влияет на эмоции получателя. Например, это может быть оповещение о большом выигрыше или же, наоборот, сообщение о взломе аккаунта с дальнейшим предложением перейти по фишинговой ссылке и ввести данные авторизации. Пользователь переходит на предоставленный ресурс и «отдает» свой логин и пароль в руки мошенника, который, со своей стороны, достаточно быстро оперирует полученной информацией.

- **Пример фишинга**

Возьмем в качестве примера популярную социальную сеть **«Facebook»**. Допустим, хакер создал страницу, которая идеально похожа на страницу входа в систему **«Facebook»**, но изменил ее URL-адрес. Например, fakebook.com или faecbook.com или любой другой URL-адрес, который очень похож на оригинальный. Пользователь, попадая на такую страницу, может не обратить внимания на неверный адрес страницы из-за схожего написания адреса страницы с оригиналом. И может принять данную фишинговую страницу за настоящую страницу входа в **«Facebook»**, и без опаски воспользуется регистрационной формой для входа в систему.

Таким образом, пользователь, который не заметил разницы и воспользовался поддельной страницей, мог ввести свои регистрационные

данные и дать доступ мошеннику к своему аккаунту. Одновременно с этим, для сокрытия мошенничества, пользователь будет перенаправлен на исходную страницу **«Facebook»**.

Рассмотрим возможный пример из жизни: Игорь работает программистом и написал программу, позволяющую получить доступ к регистрационным данным пользователя. Затем он создает поддельную страницу входа в социальную сеть **«Facebook»**, содержащую вредоносную программу, и размещает ее на **«https://www.facebouk.com/money-online»**. У Игоря есть друг Павел. И Игорь отсылает Павлу сообщение: **«Привет, Паша, я нашел способ легкого заработка в интернете. Ты обязательно должен его увидеть на https://www.facebouk.com/money-online»**. Павел переходит по ссылке и видит перед собой стандартную страницу входа в систему **«Facebook»**. Как обычно, он вводит свои имя пользователя и пароль. Теперь все регистрационные данные пересылаются Игорю, а Павел перенаправляется на страницу с советами по заработку денег в сети интернет **«https://www.facebouk.com/ money-online.html»**. Вот и все, аккаунт Павла в **«Facebook»** был взломан.

- **ЧАЩЕ ВСЕГО ПОДДЕЛЫВАЮТ САЙТ ТОРГОВОЙ ИНТЕРНЕТ-ПЛОЩАДКИ «KUFAR» И ПОЧТОВОГО СЕРВИСА «БЕЛПОЧТА», А ТАКЖЕ И ОСТАЛЬНЫХ САЙТОВ НА КОТОРЫХ НЕОБХОДИМО ВВОДИТЬ ЛИБО ЛОГИН И ПАРОЛЬ ОТ УЧЕТНОЙ ЗАПИСИ ЛИБО РЕКВИЗИТЫ БАНКОВСКОЙ ПЛАТЕЖНОЙ КАРТЫ.**

КАК ЗАЩИТИТЬСЯ ОТ ДАННЫХ ВИДОВ МОШЕННИЧЕСТВА?

Как не попасться на крючок охотников за наживой? Прежде всего, следует всегда придерживаться следующих рекомендаций при использовании интернета и любых других ресурсов связи:

- всегда обращайте внимание на отправителя и тему сообщения. Если они выглядят подозрительно, просто удалите письмо;
- в письме с неизвестным отправителем не стоит переходить по предложенным ссылкам;
- ни в коем случае не давайте ответы на письма, запрашивающие личную информацию;
- следите за ошибками в тексте, если они есть, то скорее всего письмо – обман;
- файлы, прикрепленные к письму, имеющие расширения .exe, .msi, .bat, .pif, .com, .vbs, .reg, .zip могут устанавливать вредоносное программное обеспечение, не стоит их открывать.

Что касается технических средств защиты от фишинга, то не лишним будет обратить внимание на следующие возможности:

- В основных браузерах – Mozilla Firefox, Google Chrome, Microsoft Edge, Safari существует антифишинговая система со списком сайтов злоумышленников, которая предупреждает пользователя о переходе на вредоносный сайт. Такие же системы используют и многие ресурсы, по типу социальных сетей.
- Антивирусное программное обеспечение дает довольно надежную защиту. Следует всего лишь вовремя устанавливать обновления, которые дают возможность предотвратить внедрение вирусов на конечное устройство, а также оповещают пользователя об опасности при переходе по вредоносным ссылкам.
- Некоторые спам-фильтры, используемые сервисами электронной почты, позволяют автоматически отсеивать письма злоумышленников.
- Обязательно используйте двухфакторную аутентификацию. Если все ваши аккаунты будут дополнительно защищены одноразовыми паролями, это в разы усложнит жизнь злоумышленникам. Время жизни одноразового пароля ограничено — не более 60 секунд, значит, чтобы получить доступ к учетной записи пользователя, фишеру нужно быть более изобретательным и быстрым. Не так легко выудить и логин, и пароль, и одноразовый пароль, да еще и успеть войти в аккаунт атакуемого или провести нелегальную транзакцию за такой короткий промежуток времени.

3) Как взламывают страницу?

Сначала злоумышленники вычисляют логин пользователя. Его не трудно определить, обычно он состоит из адреса электронной почты или номера телефона. Такую информацию они узнают у друга, уже взломанной страницы. Остается только подобрать пароль, который вычисляется банальным подбором букв и цифр. В интернете существуют программы, которые автоматически взламывают до 70% паролей.

Распространенные аферы в сети Интернет:

От взлома аккаунта никто не застрахован. Из-за своей невнимательности пользователи соцсетей, сами того не понимая, отдают личные данные мошенникам. Способов завладеть чужим профилем достаточно.

- Просьба о финансовой помощи

Войдя на взломанную страницу, аферисты делают рассылку друзьям с просьбой выслать денег. Начинают вести переписку в сообщениях так, чтобы их не заподозрили. Интересуется делами, обращаются по имени,

располагают жертву к диалогу. Как только общение налаживается, под разными предлогами просят определенную сумму в долг: на лечение, скинуть на телефон, одолжить до завтра и т. д. Некоторые доверчивые граждане пересылают деньги на счет злоумышленника.

Как себя вести, чтобы не попасть в ловушку. Прежде чем пересылать деньги, нужно убедиться, что сообщения пишет настоящий друг или подруга: задать вопрос или спросить информацию, известную только вам и другу; не спешить переходить по сомнительным ссылкам, пересланным в личные сообщения; позвонить хозяину страницы и уточнить, нужна ли на самом деле помощь.

Если информация не подтверждается, взломанному пользователю сайта срочно обратиться в службу техподдержки Одноклассников или Вконтакте. Попытаться изменить пароль в электронной почте, если она привязана к странице социальной сети.

- Взломщик от имени друга пишет сообщение, в котором заводит стандартный разговор, интересуется делами и новостями, происходящими в жизни. Потом просит номер телефона, якобы записать на всякий случай. Добродушные друзья, ничего не подозревая, отсылают его. Через несколько минут снова приходит сообщение с просьбой сказать шестизначный код, который пришел на телефон. Как только код получен, доступ на страницу для злоумышленников открыт.
- Аферисты присылают сообщения, содержащие ссылку. Под ней может быть написано, что это подарок или новое фото, которое просят оценить. Пользователю становится интересно, он на нее кликает, тем самым все данные браузера с логинами и паролями отправляются в руки киберпреступников. Доступ на страницу для жертвы закрыт, ее уже начинают использовать в мошеннических целях.
- Преступники используют точную копию сайта социальных сетей, но с неверным адресом. Жертве приходит на почту письмо с интригующим началом какой-нибудь статьи или истории, под ней находится ссылка. Чтобы почитать дальше, нужно на нее нажать. Появляется окошко для введения логина и пароля или просьба авторизоваться через определенную социальную сеть. Таким образом, личные данные попадают на фальшивый сайт злоумышленников.

Вывод один: жертвой обмана может стать любой человек, пользующийся социальными сетями. Чтобы обезопасить аккаунт от взлома, нужно чаще менять пароль. Лучше, чтобы он состоял из несуществующего слова, которое будет понятно только хозяину страницы. Не раздавать номер телефона, а тем более секретный код, подозрительным контактам.

Основные термины, используемые при совершении кибермошенничеств.

Аутентификация – процесс установления личности пользователя при попытке получения доступа к компьютеру или к файлам.

Банк-эмитент или эмиссионный **банк** — **банк**, выпускающий в обращение (эмитирующий) денежные знаки или ценные бумаги и платёжно-расчётные документы (банковские карты, чековые книжки). Эмиссией денег в стране чаще всего занимаются центральные **банки**, выпуском ценных бумаг — коммерческие **банки**. Выпущенные **банком** банковские карты на протяжении всего срока действия остаются собственностью **банка-эмитента**, а держатель карты получает её лишь в пользование.

Банк-эквайер (обслуживающий **банк**) – кредитная организация, организующая точки приема банковских карт (терминалы, банкоматы) и осуществляющая весь комплекс финансовых операций, связанных с выполнением расчетов и платежей по банковским картам в этих точках.

Ботнет или сеть ботов – это компьютерная сеть, состоящая из большого количества компьютеров, на которых скрытно установлено вредоносное ПО, позволяющее злоумышленникам удаленно выполнять любые действия с использованием вычислительных ресурсов зараженных машин. Сотни или даже тысячи зараженных компьютеров, как правило, используются для нелегальной и вредоносной деятельности – рассылки спама, вирусов, похищения личных данных или проведения DoS-атак.

Бра́узер, или веб-обозрева́тель — прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач. В глобальной сети **браузеры** используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов.

Вишинг – один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или

стимулируют к совершению определенных действий с карточным счетом/платежной картой.

Вредоносное программное обеспечение (Вредоносное ПО) – программное обеспечение, направленное на выполнение несанкционированных вредоносных действий на компьютере.

Дропы – люди, используемые для совершения противозаконных действий в качестве подставных лиц. Нередко можно встретить подобные предложения на различных форумах, досках объявлений.

Вся суть дропа заключается в совершении каких-либо незаконных действий от своего имени. При этом человек не знает, что конкретно может произойти. Все делается мошенниками, которым вы передали какие-то привилегии на осуществление операций.

Дроповоды – это те люди, которые занимается дропами, руководят ими и "водят" их. **Дропы**, в свою очередь – это подставное лицо в различного рода мошеннических схемах, промежуточное звено мошеннической схемы.

Мошенничество с платежными картами, **кардинг** (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтверждённая её держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера).

Кибератака — или хакерская атака — это вредоносное вмешательство в информационную систему компании, взлом сайтов и приложений, личных аккаунтов и устройств. Главные цели — получить выгоду от использования этих данных или шантажа владельцев.

Кибербуллинг – это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала. Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством

выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Ливанская петля – мошенничество, которое предполагает изъятие карты у её владельца (держателя) весьма бесхитростным способом. Если большинство вариантов мошенничества с банковскими картами имеют цель лишь получить их реквизиты при помощи различных программно-аппаратных ухищрений (например, скимминг или фишинг) для последующего опустошения счетов, то цель этого способа – получение самой пластиковой карты.

В картридер банкомата мошенник помещает так называемую «ливанскую петлю», которая представляет собой блокиратор из фотопленки (что-то вроде ловушки). Пользователь банковских услуг, вставляя карту в банкомат, в реальности вставляет ее в заранее подготовленный «конверт» из пленки, в котором она «благополучно» застревает.

Естественно, владелец застрявшей карточки начинает переживать и пребывать в легкой панике.

Как правило, в этот момент “неравнодушный человек” находится рядом (возможно, он даже будет переодет в форму сотрудников банка) и предлагает проделать ряд операций для спасения карточки, в том числе повторить ввод пин-кода.

Естественная паника клиента банка, «квалифицированный советчик», который «случайно» оказывается рядом и активно пытается помочь – все ведет к тому, что в определенный момент, клиент банка набирает пин-код при мошеннике. Результат: банковская карта находится в заранее установленной «ловушке», а пин-код становится известен мошеннику. После всех манипуляций мошенник советует составить заявление о возврате карты в отделении банка. Как только владелец карты уходит от банкомата, мошенник оперативно извлекает карту вместе со своим «конвертом» из пленки. Несколько минут – и карта оказывается полностью пустой.

Несанкционированный доступ — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Нигерийские письма — это один из распространённых видов мошенничества, главной особенностью которого являются массово рассылаемые электронные **письма** с душещипательными историями, в

любой из которых есть несчастный, но богатый главный герой, есть его родственники, есть огромная сумма денег, а получатель такого **письма**, чудесным образом имеет возможность всем помочь и при этом сказочно разбогатеть!

Социальная инженерия — это совокупность психологических и социологических приемов, методов и технологий, которые позволяют получить конфиденциальную информацию. Кибермошенников, которые используют эти приемы на практике, называют социальными инженерами. Пытаясь найти доступ к системе или ценным данным, они используют самое уязвимое звено — человека, который считается наименее устойчивым к внешнему воздействию.

Сватинг — тактика домогательства, которая заключается во введении аварийно-спасательной службы в заблуждение так, чтобы по адресу другого лица выехали спасательные службы. Это делается с помощью фальшивых сообщений о серьёзных правонарушениях, такие как закладки бомбы, убийство, захват заложников или другие подобные инциденты.

Скиммер – это самодельный считыватель магнитной ленты. Мошенники прикрепляют его к картоприемнику банкомата.

Сетево́й **тра́фик**, или **интерне́т-тра́фик** (англ. **traffic** — «движение», «грузооборот»), — объём информации, передаваемой через компьютерную сеть за определённый период времени.

Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего.

Хакинг – внесение изменений в программном обеспечении, для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения являются вредоносными.

Человека, занимающегося хакингом, называют **хакером**. Это, как правило, опытный программист, считающий взлом искусством, способный применить отличные навыки в реальных жизненных ситуациях. Однако,

существуют и другие хакеры, которые имеют более опасные мотивы, чем просто демонстрация своего мастерства. Они направляют свои знания на кражу личной информации, несанкционированный доступ и тому подобное.

Что такое реквизиты банковской карты?

Реквизиты — это данные банковского счета, часть из которых указана на самой карте. Чтобы полностью раскрыть информацию о безопасности системы индивидуальных расчетов, отнесем к реквизитам и секретный код карты, который дает доступ к профилю пользователя, а также банковский счет, к которому она привязана. Данные на карте включают:

- Номер банковской карты. Это 16 или 18 цифр, которые указаны на лицевой части. В номере зашифрованы название платежной системы, идентификационный номер вашего банка, тип и регион выпуска карты, системное проверочное число. Важно! В процессе проведения ряда денежных операций могут запрашивать не весь номер карты, а только 4 последние цифры.
- Имя держателя карты. Может быть указана только фамилия, фамилия и инициалы или карта может быть неименной.
- Три цифры на обороте карты. CVC2 или CVV2 — трехзначный код безопасности на обратной стороне карты, который служит для дополнительной защиты от хищений.
- Срок действия. В формате месяц/год.
- Также иногда требуется расчетный счет. Номер банковского счета, который указывается договоре на обслуживание карты или в онлайн-банке. На самой карте его нет.
- PIN-код. Четырехзначный пароль, который дает доступ к счету и операциям по карте. PIN устанавливает владелец при оформлении. На самой карте его нет и передавать его никому не нужно.

Шиммер - это тонкая «прокладка», которая располагается между чипом на карте и считывающим устройством чипов в банкомате или терминале – и записывает данные с чипа, когда их считывает терминал.

DoS-атака или **атака** Denial-of-Service (отказ в обслуживании) - это метод, используемый для нарушения доступа добросовестных пользователей к выбранной сети или веб-ресурсу. Как правило, это достигается путем перегрузки цели, (часто веб-сервера) огромным количеством трафика или путем отправки вредоносных запросов, которые приводят к отказу или к сбою работы целевого ресурса.

IP-адрес – это уникальный адрес, идентифицирующий устройство в интернете или локальной сети. IP означает «Интернет-протокол» – набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть.

По сути, IP-адрес – это идентификатор, позволяющий передавать информацию между устройствами в сети: он содержит информацию о местоположении устройства и обеспечивает его доступность для связи. IP-адреса позволяют различать компьютеры, маршрутизаторы и веб-сайты в интернете и являются важным компонентом работы интернета.

Tor — это сервис для анонимного доступа в интернет и, как следствие, обхода блокировок. Через Tor можно зайти на любой заблокированный ресурс.

VPN (англ. Virtual Private Network — виртуальная частная сеть) — это безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность.

Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Дословно Wi-Fi переводится – беспроводное качество.