**1) Что такое киберпреступность? Защита от киберпреступности.**

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Киберпреступления совершают частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически.

Для примера можно привести некоторые разновидности киберпреступлений:

* мошенничество с использованием электронной почты и интернета;
* кража цифровой личности (хищение и использование личных данных);
* кража данных платежных карт и другой финансовой информации;
* хищение и перепродажа корпоративных данных;
* кибершантаж (вымогательство денег под угрозой атаки);
* атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа);
* криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);
* кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);
* нарушение работы систем с целью компрометации сети;
* нарушение авторских прав;
* незаконное проведение азартных игр;
* онлайн-торговля запрещенными товарами;
* домогательства, изготовление или хранение детской порнографии;

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности:

1) Повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.).

2) Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств.

3) Особая подготовленность преступников, интеллектуальный характер преступной деятельности.

4) Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств.

5) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления.

6) Многоэпизодный характер преступных действий при множественности потерпевших.

7) Неосведомленность потерпевших о том, что они подверглись преступному воздействию.

8) Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

9) Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Примеры кибератак:

- атаки с использованием вредоносных программ;

- фишинг (отправка спама (в электронных письмах или по другим каналам), чтобы обманным путем вынудить пользователей сделать нечто, что ослабит их безопасность. Фишинговые сообщения могут содержать зараженные вложения, ссылки на вредоносные сайты или просьбу предоставить конфиденциальную информацию.

- распределенные DoS-атаки (нацелены на вывод из строя какой-либо системы или сети. Иногда для проведения DDoS-атак используются устройства IoT (интернета вещей).

Способы защиты от киберпреступлений:

- регулярное обновление ПО и операционной системы;

- использование антивирусных программ и их регулярное обновление;

- использование надежных паролей;

- привычка не открывать вложенные файлы в письмах;

- привычка не переходить по ссылкам в спам-письмах и на недоверенных веб-сайтах;

- осторожность при передаче личной информации;

- общение по официальным каналам;

- внимательность при посещении веб-сайтов;

- регулярная проверка банковских выписок.

помощник прокурора

г. Буйнакска

юрист 1 класса Н.А. Магомедова

**2) О вопросах противодействия преступности в сфере использования информационно-коммуникационных технологий.**

Мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием, в том числе совершенное дистанционным способом с использованием информационно-коммуникационных технологий, в современном обществе является одним из самых распространенных видов преступлений.

Указанный вид мошенничества совершается как правило без физического контакта с потерпевшим.

Способы совершения хищения с использованием информационно-коммуникационных технологий постоянно совершенствуются, что создает определенные сложности для правоохранительных органов в раскрытии преступлений указанной категории.

Одним из самых распространенных видов хищения является телефонное мошенничество. Как правило, от имени сотрудников банков России, мошенники сообщают потерпевшему о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимой блокировки банковской карты. Далее, мошенники, войдя в доверие, просят предоставить определенные данные карты владельца или сообщить смс-код, поступивший на его телефон. В результате чего, как правило, происходит списание денежных средств с банковского счета.

Нужно помнить, что сотрудники банка при общении с клиентом банка никогда не просят сообщить ему реквизиты банковской карты.

Зачастую мошенники могут представиться сотрудниками полиции и сообщают о том, что близкие родственники задержаны за совершение преступления либо стали виновниками дорожно-транспортного происшествия, в результате которого погибли люди. Для того, чтобы родственник избежал наказания мошенник предлагает заплатить определенную сумму денег. В последнее время участились случаи, когда за денежными средствами приезжают курьеры, либо мошенники просят перевести денежные средства через платежный терминал.

Также, довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае мошенники, с помощью взлома персональной страницы в социальных сетях, обращаются от лица потерпевшего с просьбой о помощи, а именно о переводе денежных средств на банковский счет, либо просят реквизиты карт, чтобы перевести деньги.

Мошенничество через «Интернет-магазин» - еще один способ обмана. Преступники берут с будущей жертвы предоплату или полную сумму за определенный товар, но не исполняют своих обязательств. Благодаря фальшивых интернет-сайтов, мошенники собирают реквизиты банковских карт потерпевших и далее используют для операций по обналичиванию денежных средств.

Будьте внимательны и осторожны при общении с посторонними лицами.

**Подробнее см. Семейный кодекс Российской Федерации, Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве».**

Помощник прокурора г. Буйнакска

юрист 1 класса Н.А. Магомедова

**3) Последовательность действий при взломе профиля на «Госуслугах».**

Как восстановить доступ? Для начала попробуйте сбросить старый пароль с помощью почты или по номеру телефона. Для этого на странице авторизации выберите «Восстановить». Затем введите телефон или e-mail и номер одного из документов: паспорта, ИНН или СНИЛС.

Не получилось войти с помощью номера телефона? Попробуйте вариант с адресом электронной почты. И наоборот.

Или восстановите доступ в одном из центров обслуживания клиентов «Госуслуг» (https://map.gosuslugi.ru/?layer=co).

Доступ удалось восстановить. Что нужно проверить?

Когда аккаунт снова в ваших руках, важно перекрыть мошенникам доступ к вашему профилю, а также выяснить, какие именно данные их интересовали.

1. Первым делом зайдите в своем профиле в раздел «Безопасность». В подразделах «Мобильные приложения» и «Действия в системе» выйдите из аккаунта со всех устройств, кроме того, которым вы сейчас пользуетесь.

2. Проверьте, правильно ли указаны телефон и почта в графе «Учетная запись». Поменяйте телефон на свой. Если у вас стандартная или упрощенная учетная запись, для смены номера потребуется ввести код подтверждения, который придет в СМС от портала.

3. В разделе «Безопасность» в подразделе «Действия в системе» посмотрите, на каких ресурсах проходили авторизации через ваш профиль. Например, злоумышленники могли использовать ваш аккаунт для входа в личный кабинет банка или микрофинансовой организации МФО. В таком случае срочно свяжитесь с финансовой организацией. Скажите, что ваш профиль взломали. Выясните, что происходило с вашими счетами за последнее время и не появилось ли у вас новых кредитов и займов.

4. Сообщите о случившемся в техподдержку «Госуслуг» и в полицию.

Передайте все известные вам подробности: время взлома, чужие контактные данные, которые появились в аккаунте вместо ваших. Сохраните копию заявления в полицию и талон-уведомление о его приеме. Если мошенники наберут долгов на ваше имя, будет проще доказать, что займы брали не вы.

5. Периодически проверяйте свою кредитную историю – данные обо всех ссудах на ваше имя. Так вы быстро узнаете, если мошенникам все-таки удастся взять займы на ваше имя, и сможете их оспорить.

Чтобы предотвратить взлом профиля в дальнейшем, задайте сложный пароль и не забывайте время от времени обновлять его.

Помощник прокурора г. Буйнакска Магомедова Н.А.

**4) Что такое спуфинг и как от него защититься?**

Спуфинг - кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации. Подмена может происходить через Интернет-сайты, электронную почту, телефонные звонки, текстовые сообщения, IP-адреса и серверы.

Основная цель спуфинга - получить доступ к личной информации, украсть деньги, распространить вредоносное программное обеспечение.

Типы спуфинг-атак:

-Подмена номера - мошенник использует ложную информацию для изменения идентификатора вызывающего абонента т.е. мошенник звонит якобы с другого телефона – например, телефон вашего друга.

-Подмена сайта - мошенник пытается создать опасный (вредоносный) сайт похожим на надежный безопасный сайт (например, известного банка), используя его шрифты, цвета и логотипы.

-Подмена почты - мошенник рассылает электронные письма с поддельными адресами отправителей с намерением заразить ваш компьютер вредоносными программами, заполучить деньги или украсть информацию. В качестве адресов электронной почты отправителей зачастую подставляются те адреса, которым вы можете доверять.

-Подмена IP-адреса - мошенник стремится скрыть реальное местоположение в Интернете того места, откуда запрашиваются или куда отправляются данные пользователя, чтобы заставить компьютер жертвы думать, что информация, отправляемая мошенником пользователю, исходит из надежного источника, что позволяет вредоносному контенту доходить до пользователя.

-SMS-спуфинг - мошенник отправляет текстовое или SMS-сообщение, используя номер телефона другого человека.

Существует ряд рекомендаций, которым следует придерживаться, чтобы защитить себя от спуфинг-атак:

- Включайте спам-фильтр: это предотвратит попадание большинства поддельных писем в ваш почтовый ящик;

- Изучайте сообщения: грамматические ошибки или необычная структура предложения;

- Подтвердите информацию: если электронное письмо или звонок кажутся подозрительными, отправьте сообщение или позвоните отправителю, чтобы проверить, является ли полученная информация действительной;

- Используйте антивирусное программное обеспечение.

В случае совершения в отношении вас мошеннических действий незамедлительно обращайтесь в правоохранительные органы.

Помощник прокурора г. Буйнакска Магомедова Н.А.

**5) Что такое вишинг и как от него защититься?**

Вишинг — это вид интернет-мошенничества, при котором злоумышленники, используя телефонную коммуникацию, под разными предлогами вынуждают людей совершать действия якобы в их собственных интересах.

С этой целью злоумышленники рассылают сообщения с вредоносными ссылками. После перехода по ссылке отображается синий экран с предупреждающим сообщением и бесплатным номером телефона, по которому следует позвонить для устранения серьезной проблемы с компьютером.

На звонок отвечает вежливый технический специалист, который готов оказать вам любую помощь за деньги. После того, как пользователь предоставит информацию о своей кредитной карте для оплаты программного обеспечения, необходимого для решения проблемы с компьютером, мошеннические действия завершаются.

При этом программное обеспечение не работает, вежливый технический специалист исчезает, как и денежные средства. А пользователь становится еще одной жертвой мошенничества, называемой «вишинг».

Как распознать вишинг? Есть предупреждающие знаки, которые помогают распознать потенциальное мошенничество.

Во многих случаях звонящие являются самозваными экспертами или специалистами в своих областях. Они могут представляться компьютерными специалистами, банкирами, полицейскими или даже жертвами мошенничества.

Однако, если звонящие действительно те, кем они представляются, то их профессиональную принадлежность нетрудно проверить простым звонком. Если они не смогут или не захотят предоставлять информацию, необходимую для проверки их личности, доверять им нельзя. Но даже если они предоставляют контактную информацию, стоит проверить их легитимность, позвонив по официальному номеру телефона организации.

В случае совершения в отношении вас мошеннических действий незамедлительно обращайтесь в правоохранительные органы.

Помощник прокурора г. Буйнакска Магомедова Н.А.