Внимание, участились случаи интернет мошенничества!

Интернет мошенничество– один из самых распространенных видов преступления. Безопасность в интернете во многом зависит и от нас самих, применяя несложные правила можно оградить себя от мошенников.

Самые распространенные схемы интернет мошенничества:

- Злоумышленники создают фальшивые аккаунты в мессенджерах и социальных сетях, убеждая жертву передать ему личные данные (ФИО, пароль, данные банковской карты, о счетах) тем самым, списывают денежные средства с банковских счетов.
- Высылаются .apk-файлы с наименованием «Это твое фото», при этом файл содержит вредоносную программу, которая получает доступ к Вашим приложениям
- Предложения выгодного заработка (например: для того, чтобы зарегистрироваться в онлайн-подработке необходимо внести комиссию, так оплачивая комиссию вы даете мошенникам списать денежные средства с вашего счета)

Предложения о вложении денежных средств в целях увеличения дохода - инвестиций (злоумышленники предлагают вложить определённую сумму для получения пассивного дохода, после вложения денежных средств, злоумышленники якобы возвращают денежные средства с процентами, так жертва теряет бдительность и в дальнейшем вносит еще денежные средства)

- В связи с повышенной активностью злоумышленников по рассылке фишинговых электронных писем и спам-рассылок, прошу учесть следующие меры безопасности: 1. Не переходите по ссылке, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок; 2. Не нажимайте на ссылки, если они заменены на слова; 3. Не копируйте адрес ссылки; 4. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD; 5. Не подгружайте картинки от незнакомых людей; 6. Не запускайте макросы в офисных приложениях (макрос - это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи.); 7. Не пересылайте письма коллегам; 8. Проинформируйте администратора безопасности – главного специалиста отдела правовой статистики и защиты информации прокуратуры республики Ондар Л.Ч., направив ему полученное письмо как вложение. 9. Удалите фишинговое письмо.

- Мошенничества с объявлениями о продаже товара и предоставлении услуг:

- злоумышленники завлекают ничего не подозревающих покупателей товарами за низкую цену, покупатели оплачивают товар, в итоге продавец получает оплату и пропадает или присылает другой товар

-оплата или предоплата, злоумышленники очень часто просят внести предоплату за товар, отправляют ссылки и требуют внести данные банковской карты, ФИО, срок действия карты, трёхзначный код на обороте карты (CVC-код), пин-код, таким образом получают доступ к вашему банковскому счету

- случайные смс-сообщения со ссылкой и файлы, **переходя по которым вы можете загрузить на свой телефон вредоносное программное обеспечение**, который позволит мошенникам получить доступ к вашим банковским счетам (например: Сообщения содержащие сведения о начислении скидок, бонусов, рекламу).

Под видом сотрудником ОМС под предлогом необходимости замены медицинского полиса получают доступ к Госуслугам

Прокуратура г. Кызыла предупреждает граждан быть бдительными и соблюдать элементарные правила безопасности, чтобы не стать жертвой мошенников:

Не вводите на сомнительных сайтах личные данные и данные банковских карт.

Покупайте товары только на проверенных сайтах и интернет-магазинах.

Не переходите по сомнительным сайтам, ссылкам и не устанавливайте сомнительные приложения.

Не сообщайте свои персональные данные НИКОМУ.

В случае если Вы все-таки стали жертвой мошенника необходимо незамедлительно обратиться в правоохранительные органы по тел: 9-36-01, 9-36-02

Внимание, телефонные мошенничества!

Мобильные телефоны стали неотъемлемой частью нашей жизни, отвечая на звонки, мы, не задумываясь начинаем разговор с незнакомым собеседником. Этим пользуются и злоумышленники! Они постоянно придумывают разные схемы обмана для того, чтобы выманить у своих жертв деньги или конфиденциальные данные для доступа к банковским счетам.

К телефонным мошенничествам относятся:

- Звонки от «банковских служб безопасности, сотрудников Центрального Банка, сотрудников вашего банка», злоумышленник по телефону сообщает о подозрительной операции по Вашей банковской карте (счету) или получении кем-то от Вашего имени кредита. Говоря о том, что кто-то пытается оформить на Вас кредит, предлагают опередить мошенника и вывести деньги с банковского счета, однако действуя по инструкции мошенника, Вы оформляете кредит на свое имя и переводите денежные средства мошеннику! Или же могут сообщить о том, что, по-вашему счету уже проведена подозрительная операция, а для ее отмены нужно назвать код из СМС, а также реквизиты банковской карты (номер, срок действия, трехзначный код на обороте карты).
- Звонки с фальшивых номеров, так злоумышленники используют специальные программы, которые подменяют их номера на официальный номер какого-нибудь банка, например номер «Сбербанка» и также сообщают о подозрительных операциях.
- Звонки от «сотрудников правоохранительных органов, МВД, ФСБ, прокуратуры» в этом случае, злоумышленники сообщают, что вы стали жертвой преступления и преступники пытаются перевести денежные средства с вашего счета. В таких случаях, мошенники переводят звонки к так называемым «специалистам банка» для подтверждения якобы операции по Вашим счетам, которые на самом деле просто являются соучастниками.

ЗАПОМНИТЕ! Мошенники стремятся вызвать эмоции, нагнетая панику со словами **«Срочно», «Нет времени», «Быстрее»**, они не дают времени на то, чтобы обдумать свои действия, иногда переходят к уговорам.

Важно обращать внимание на то, как с Вами разговаривает собеседник!

- сотрудник банка никогда не будет разговорить с Вами в течение часа или больше, так как у них большой поток обращений;
- торопить Вас и давить со словами «Деньги надо срочно перевести на надёжный счет»;
- переводить звонок к специалистам других банков или в полицию
- сотрудники банка и правоохранительных органов никогда не просят называть банковские реквизиты и не просят перевести денежные средства на «надежный счет».

Что же делать в том, случае если вам позвонили мошенники?

1. Не отвечайте и не перезванивайте, если это неизвестные номера
2. Не сообщайте никому свои персональные данные, данные о банковских счетах и номера карт.
3. Не переходите по ссылкам, которые вам отправляют во время звонка.
4. **Проверяйте всегда информацию и никогда не принимайте поспешных решений. Берите паузу, сбрасывайте звонок и звоните на горячую линию ВАШЕГО банка! Сходите в отделение Вашего банка!**

ПРОКУРАТУРА Г. КЫЗЫЛА ПРЕДУПРЕЖДАЕТ, КАК НЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЯ!

В настоящее время около 70 % от всего количества зарегистрированных краж совершены в общественных местах. Основным предметом преступных посягательств является сотовый телефон, немного реже деньги и другие ценности.

Большое скопление людей в автобусе или очередь в магазине, способствуют кражам из карманов, сумок, однако уберечься от злоумышленников возможно, если Вы будете внимательными в переполненном автобусе, при посещении магазина или других многолюдных мест

При этом следует соблюдать несколько правил, находясь в общественном месте:

- следить за своим имуществом, перед движением по салону убирать телефон и деньги во внутренние карманы сумок или верхней одежды, держа сумки в закрытом виде и перед собой.
- проявлять особую бдительность в момент посадки (часто злоумышленники пользуются тем, что в момент посадки люди толкаются).
- не доставать телефоны и ценные вещи без надобности.
- без необходимости также не стоит брать с собой крупные суммы денег.
- не стоит хранить в чехле телефона банковские карты и пин-коды.
- детям и подросткам рекомендуется носить телефон в закрытом ранце или рюкзаке, сняв их и держа перед собой.
- обращайте внимание на людей, которые пытаются подойти к Вам поближе, встают сзади или сбоку.
- сидя в кафе, не оставляйте кошелек или иные ценные вещи в карманах одежды, даже если она висит на спинке вашего стула (нередко злоумышленники преднамеренно занимают соседнее место, вешают одежду рядом с вашей, что позволяет отвлечь ваше внимание)

В случае если все же карманнику удалось похитить ваше имущество, то Вам необходимо:

- ✓ Запомнить приметы внешности злоумышленника (во что был одет, примерный рост, возраст, телосложение);
- ✓ В каком направлении скрылся преступник:
- ✓ Незамедлительно сообщить в ДЧ УМВД России по г.Кызылу **по тел: 9-36-**

Прокуратура г. Кызыла предупреждает граждан быть бдительными и соблюдать элементарные правила безопасности, принимать все необходимые меры для сохранности своего имущества.