Информация для ознакомления.

Все мы пользуемся услугами сотовой связи и ИНТЕРНЕТОМ. К сожалению, далеко не все люди знают о том, что интернет является тем местом, где вы можете лишиться своих личных накоплений. (а если и знают, то в нужный момент забывают об этом).
В ИНТЕРНЕТЕ мошенничество приобрело массовый характер. Особенностью данного вида преступлений является то, что в большинстве случает жертва **добровольно и сознательно** предоставляет преступнику информацию, деньги или имущество.

«Новые» виды мошенничества появляются достаточно часто. В среднем одна конкретная схема мошенничества существует от 3 до 24 месяцев. В данной рекомендации материал будет изложен в простой, утрированной форме, но этого будет достаточно, чтобы не стать очередной жертвой интернет-мошенничества. Данные рекомендации помогут вам понять простые правила при использовании средств связи и информационно-телекоммуникационной сети «Интернет».

Рекомендации:

1) СМС-код.

С различных интернет-ресурсов для подтверждения личности или аутентификации вам на сотовый телефон могут приходить одноразовые СМС коды. ЗАПОМНИТЕ! Данные СМС коды никому сообщать НЕЛЬЗЯ.
В самом сообщении как правило, приходит текст со следующим содержанием: **«Код для входа 1234. Никому не сообщайте данный код» или «Никому не сообщайте этот код для подтверждения: 1234»**
Для мошенников – получение СМС-кода является только первым этапом при совершении в отношении вас противоправных действий.
Написано не сообщать код никому – не сообщайте!

2) Фишинговые сайты.

Мошенники подделывают все. Сайты крупнейших транснациональных корпораций, маркетплейсов, различных муниципальных, региональных и федеральных служб, ведомств и т.д. и т.п.
Основная задача сайта – получить ваши персональные данные (ФИО, дата рождения, сведения о паспорте, абонентский номер телефона, клиентом какого банка вы являетесь, номер вашей банковской карты/счета, срок действия карты, CVV-код, СНИЛС, ИНН, место вашей работы и прочее) – все эти данные в большинстве случаев вы предоставляете мошенникам **добровольно, хоть и не знаете об этом.**
Идеального способа проверки сайта нет, но рекомендуется:

- проверять адрес сайта
- обращать внимание на орфографические ошибки текста на самом сайте
- обращать внимание на отсутствие контактной информации, пользовательских соглашений
- обращать внимание на необоснованные требования или запросы на получение ваших личных данных.

Чтобы не стать жертвой интернет-мошенничества нужно использовать «критическое мышление».

Пример: (в адресной строке сайта указано: https://www.ozonn.ru или https://www.wildberies.ru)
Лишняя или недостающая буква, цифра, символ – это фишинговый сайт. Не увидели, воспользовались услугами данного сайта, указали свои анкетные данные –**Предоставили сведения о себе**. Указали банковские реквизиты на данном сайте – **с большой долей вероятности будет осуществлён перевод денежных средств.**

3) Инвестиции.

В интернете вы будете находить разные сомнительные предложения по инвестированию/вложению своих средств с целью получить проценты/доход/комиссионное вознаграждение за свои усилия/действия и т.д.
В данном направлении у мошенников есть несколько направлений:

- Ценные бумаги, акции, облигации, фонды ликвидности, ПИФы и т.д.
- биткоин, эфир, ЮЗДТ (USDT) и т.д.
- выкупы товаров на маркетплейсах
- написание текстов/сайтов
- переводы на русский язык
- различные разовые предложения о работе/фрилансе
- прочее

Особое распространение у мошенников получило инвестирование в «ценные бумаги на российском фондовом рынке», т.к. это направление деятельности современное и преподносится в рекламе как достаточно легкий способ заработать.

Пример: (нашли сайт/организацию/канал в мессенджере/группу в социальной сети и т.д. на тему «инвестиций», «брокерские услуги»)
Проверьте данную организации на общедоступных ресурсах!
Конкретно в данном примере – **брокер** – это компания-посредник между вами и фондовой биржей. Чтобы организация могла оказывать брокерские услуги, ей необходимо получить брокерскую лицензию, данную лицензию выдаёт Центральный Банк Российской Федерации (ЦБ РФ).
Посещаем сайт ЦБ РФ, далее находим «Реестры», далее «Список брокеров».

Дополнительно.

1) Если вы потеряли/сломали/не пользуетесь сим-картой, оформленной на ваше имя и к данному абонентскому номеру у вас «привязан» личный кабинет мобильного приложения банка – СХОДИТЕ В БАНК и УВЕДОМИТЕ БАНК о смене/утрате абонентского номера. **Это ваша обязанность! Это прописано в договоре с банком!**
Если в отношении вас будут совершены мошеннические действия и будет установлено, что использовался ваш старый (неактуальный) абонентский номер, а также что вы ранее уведомили банк о смене абонентского номера, то для вас утрата денежных средств не будет проблемой, банк вам все возместит, т.к. вы выполнили условия договора и в нарушении безопасности и сохранности ваших накоплений виновата коммерческая организация.

2) Заведите/закажите себе отдельную банковскую карту, которую вы будете использовать для совершения покупок в интернете. Переводите на неё нужное количество средств для совершения операций.
Данная рекомендация не является защитой на все 100%, но как минимум поможет вам ограничить размер причиненного ущерба. Мошенники смогут совершить хищение только на сумму, которая будет находится на данной банковской карте.
Это не должна быть **КРЕДИТНАЯ КАРТА**. Обычная дебетовая карта банка, клиентом которого вы являетесь.

3) **Страховка от мошенничества.**
Большинство финансовых организаций (банков) предлагают услуги по страхованию от мошенничества. Страховые суммы и стоимость услуги у всех разная.
В достаточной степени, является действенной мерой при страховании возрастной группы населения, т.к. они подвергаются влиянию мошенников – чаще всего.

4) У большинства есть дети.
   - Устанавливайте функции ограничения контента: «безопасный интернет», «детский интернет», «детский оператор», «защита от спама» и т.д. (данные функции доступны у сотовых операторов, а также у финансовых организаций)
   - Устанавливайте ограничения по расходам в финансовых организациях (лимит в день, месяц и т.д.)

5) Дроп-карты.
В среде интернет можно встретить объявления на тему «куплю карту», «куплю кредитку», «куплю карты оптом» и т.д., данные объявления распространяют пособники мошенников.
В большинстве случаев на такие объявления реагируют дети, подростки, люди с финансовыми трудностями и т.д.
Несколько лет назад за продажу банковской карты можно было получить 2500 рублей, сейчас более 20000 рублей.
Спрос на данную услугу растет, следовательно необходимо уделить данной теме немного времени.
Запомните и разъясните своим детям, родственникам, друзьям, знакомым:
Если вы продали карту, то вероятнее всего через данную карту будут проводится сомнительные (незаконные) операции.
В большинстве случаев, для **продавца** банковской карты это не несет **уголовную ответственность**, но это не отменяет ответственность в гражданско-правовом порядке.