Как защититься от кибермошенничества.

В данной статье рассмотрим популярные схемы мошенничеств и используемые аферистами инструменты.

1. «Безопасный счет» или «Резервный счет». Следует запомнить, что таких понятий не существует в финансовой и банковской сфере и используется они только мошенниками. Преступники связываются с жертвой по телефону, в соцсетях или мессенджерах, выдают себя за представителей правоохранительных органов, социальных служб, банков, работников почты, энергосбыта, управляющей компании, специалистов МФЦ, портала «Госуслуг» и. т.п. с целью заставить человека перевести деньги на «безопасный или резервный счет», якобы для сохранности. В ход идут психологическое давление и манипуляции. Жертву убеждают в том, что действовать нужно прямо сейчас. Схема, казалось бы, избитая — но все еще популярная.

Как защититься? Если поступил сомнительный звонок заблокируйте его, перезвоните на горячую линию банка по номеру телефона, указанному на обороте Вашей карты и узнайте о всех последних действиях с Вашими счетами. Не доверяйте неизвестным телефонным и интернет-собеседникам — кем бы они не представлялись

2. Фишинговые сайты

Другое популярное направление интернет-мошенничества — это фишинг. Суть такова: преступники создают копию какого-нибудь интернет-ресурса: сайта банка, маркетплейса, платежной системы, интернет-магазина, социальной сети и так далее. Выдавая ее за настоящий ресурс, они собирают персональные и авторизационные данные граждан. А если удается, то и вовсе похищают чужие деньги.

Например: Василию приходит ссылка от его друга Петра со ссылкой на известный интернет-магазин, в котором по выгодной цене предлагаются смартфоны. Василий ничего не подозревая, ведь ему написал друг, переходит по ссылке и заказывает смартфон, совершая предоплату. На самом деле аккаунт Петра был взломан, и злоумышленник прислал Василию ссылку на фишинговый, поддельный сайт. В итоге деньги за «предоплату» ушли мошенникам.

Как защититься? Не переходить по подозрительным ссылкам, даже если их прислали родственники и друзья. Их аккаунты могли взломать. Вместо перехода по ссылке используйте поисковые системы.

3. Фальшивые интернет-магазины и товары на маркетплейсах

Мошенники создают поддельный интернет-магазин — на базе маркетплейса или в виде отдельного сайта и предлагают товары по крайне низким ценам. Что происходит дальше? Мошенники либо ничего не отправляют покупателю и после поступившей оплаты исчезают с радаров, либо отправляют вместо дорогой техники ее дешевые реплики или сверхбюджетные модели вместо той, за которую заплатил покупатель. Такая схема часто встречается на маркетплейсах. Периодически названия магазинов меняются. Например, когда сайт мошенников блокирует Роскомнадзор. Или когда у продавца на маркетплейсе копятся негативные отзывы.

Как защититься? Изучать отзывы о магазине (в том числе, на сторонних площадках). наличие информации о продавце, размещенной на сайте интернет- магазина, ИНН, ОГРН. Достоверность ИНН и ОГРН нужно проверять на официальном сайте ФНС России

4. Инвестиции

Согласно статистике, большинство жертв сами связываются с лжеброкерами, увидев рекламу в Интернете. В стремлении заработать за короткий промежуток времени крупную сумму денег потерпевшие переводят на указанные счета многомиллионные суммы.

Как защититься? Перепроверять информацию и критически относиться к легендам о быстром заработке. За консультацией и разъяснением следует обращаться лично к официальным представителям в отделениях банка или по телефону горячей линии.

5. Спам-рассылки

Банальные спам-рассылки все еще не утратили актуальности, часто их также рассылают от лица государственных органов, банков или известных компаний.

В качестве примера можно привести письмо якобы от «Пятерочки» со ссылкой на розыгрыш. На самом деле ссылка вела на сайт с нечитаемым названием. Для участия в розыгрыше предлагалось скачать и запустить некий файл с расширением.exe. Очевидно, что таким образом распространялось вредоносное программное обеспечение (ПО) — возможно, шифровальщик, кейлоггер или троян-вымогатель (вирусы).

Как защититься? Не переходить по подозрительным ссылкам и не запускать сомнительные исполняемые файлы.

6. Взлом аккаунта и просьбы одолжить денег

Если в соцсети или мессенджере друг просит одолжить денег, стоит насторожиться. Возможно, контроль над его учетной записью получили мошенники.

Как защититься? Позвонить человеку на личный номер. А чтобы не стать жертвой взлома — не переходите по подозрительным ссылкам. И, конечно, подключить двухфакторную аутентификацию.

7. Сообщение от «руководителя»

Схема с выдачей себя за руководителя жертвы пришла в Россию из-за рубежа. Отечественные злоумышленники успешно ее освоили. Преступники ищут людей, которые работают в различных компаниях — и могут от лица этих компаний проводить финансовые операции. Они изучают контакты жертвы, собирают информацию об их руководителе. Затем в соцсети/мессенджере создается фейковый профиль начальника. Псевдо-руководитель пишет жертве (например, главному бухгалтеру), что вскоре поступит звонок от представителя государственного органа, директора компании или кого-то еще. А также заявляет, что работнику необходимо выполнить все указания.

Признаки данной схемы:

1. В мессенджерах номер телефона «начальника» скрыт, или ранее с ним не велось переписки.
2. Абонент переадресует звонок/сообщение «специальному человеку»
3. Большая срочность.
4. Требуется абсолютная секретность.

Как защититься? Перепроверить номер, с которого поступил звонок. Связаться с руководством и рассказать о подозрительном сообщении. Не открывать письма и не переходить по ссылкам, которые вызывают у вас опасения.
Всегда перепроверять информацию, прежде чем действовать по указаниям.

8. Ложные сборы на благотворительность

В соцсетях регулярно появляются посты с призывом о благотворительности. К примеру, нужно собрать больному ребенку денег на операцию или купить корм в приют для животных. Часть подобных постов создают мошенники. Некоторые злоумышленники и вовсе копируют сообщения официальных благотворительных фондов и организаций. В них меняются лишь реквизиты.

Как защититься? Проверять документы. Изучать информацию о благотворительной организации, которой Вы хотите сделать пожертвование.

9. Трудоустройство с предоплатой

Остерегаться мошенников следует и при поиске работы — особенно в Сети. Так, до начала работы лжеработодатели просят потратиться на некие курсы, внести комиссию, приобрести платный доступ к учетной записи, оплатить подписку на программное обеспечение и т.п., предлагая при этом невероятно выгодные» условия вакансии, что мешает жертве критически

оценить ситуацию. Пример такой вакансии: работа из дома, свободный график, редактирование карточек товаров на маркетплейсах, зарплата — более 100 тысяч в месяц.

Как защититься? Если потенциальный работодатель просит что-то оплатить или кому-то перевести денег — ищите другого работодателя.

10. Обман в соцсетях и на сайтах знакомств

В Telegram существуют целые каналы и чаты, где мошенники координируют свои усилия по такому виду «развода». Выдавая себя за привлекательного потенциального партнера, мошенник втирается к человеку в доверие с целью заполучить его денежные средства. Это может быть простая просьба помочь финансово — под тем или иным предлогом. Или же покупка несуществующих билетов на какое-то мероприятие на фейковом сайте, совместный бизнес с крайне выгодными капиталовложениями. Кроме того, мошенники успешно используют в своей преступной деятельности нейросети. Например, злоумышленник может притворяться девушкой во время видеозвонка, применяя дипфейк-технологии.

Как защититься? Проявлять внимательность и здоровую недоверчивость, не делиться важной личной информацией сразу после знакомства. С подозрением относиться к любым просьбам, связанным с финансами.

11. Мошенники пишут детям в онлайн-играх.

Кроме всего перечисленного нередкими стали случаи кибермошенничества в отношении детей и подростков. Под предлогом улучшения игрового персонажа злоумышленники просят несовершеннолетних воспользоваться мобильным банком родителей и перевести деньги на сторонние счета. Иногда дети и вовсе могут оформить кредит на взрослых. Подобные случаи также уже зарегистрированы в Приангарье.

12. Цифровой рубль

В новой схеме мошенничества с цифровым рублем граждан пытаются убедить «срочно» перевести «устаревшие» деньги на специальный счет, чтобы спасти свои деньги.

Как защититься? Не принимать эмоционально-необдуманных решений, поддавшись панике, проконсультироваться со специалистам банка, перезвонив на горячую линию, либо обратившись в отделение банка.

Информация подготовлена юрисконсультом консультационного пункта для потребителей Филиала «ФБУЗ «Центр гигиены и эпидемиологии в Иркутской области» в Эхирит-Булагатском, Баяндаевском,Усть-Удинском,Осинском, Боханском, Качугском и Жигаловском районах Бочкиной Н.В. с использованием СПС «Гарант».