Как не поддаться на уловки кибермошенников

Кибермошенничество - один из видов преступлений в Интернете, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

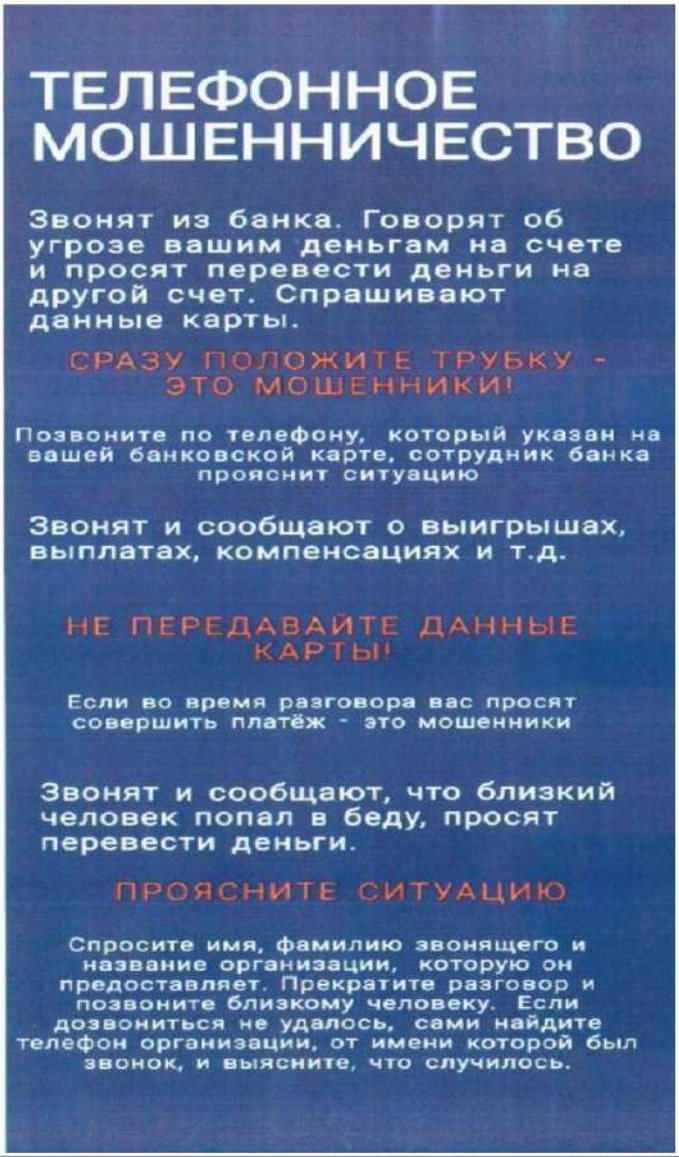
Злоумышленники для достижения целей воздействуют на эмоции, страхи и рефлексы людей и побуждают перейти по вредоносной ссылке.
При переходе по ссылке человек попадает на фишинговый сайт, где его просят ввести персональные или банковские данные.
Очень часто в сообщениях содержатся ссылки на вредоносное ПО.

В структуре **МВД России** создано специализированное подразделение – **Управление по борьбе с противоправным использованием информационно-коммуникационных технологий**, сотрудниками которого на постоянной основе проводится мониторинг ситуации.

В ходе мониторинга сети устанавливаются Интернет сайты, форумы, закрытые чаты, используемые для организации и реализации вышеуказанных преступных схем.

На информационном ресурсе данного органа можно получить необходимую методическую помощь, а также сообщить о злоумышленниках, распространяющих запрещенную или деструктивную информацию

На сайте **ГУ МВД России по г.Санкт-Петербургу и Ленинградской области** размещён доступный для восприятия тематический видео контент, содержащий как комплекс профилактических мер, так и разъясняющий способы противодействия злоумышленникам. Официальный сайт: www.78.mvd.ru. Аналогичные страницы есть в социальной сети «Вконтакте», https://vk.com/spb_police и в мессенджере «Телеграм», где размещены циклы видео-роликов, связанные со звонками со стороны лиц, действующих от имени служб безопасности банков, приобретением в сети Интернет туристических путевок и приобретением или продажей товаров и услуг на электронных торговых площадках (Авито, Юла и др.).



!!! ПОМНИТЕ !!!
Не существует 100% методик защиты от телефонного и интернет мошенничества.

Если Вы не уверены в правильности своих действий при сомнительных телефонных контактах и интернет-коммуникациях:

1) Не отвечайте на неизвестные Вам номера телефонных вызовов и СМС(ММС) запросов;

2) Не переходите по неизвестным Вам интернет-ссылкам и контактам;

3) Не пользуйтесь интернет соединением, когда он Вам не нужен на смартфоне и компьютере;

4) Не передавайте и не оставляете свои персональные данные на общедоступных ресурсах не проходите сомнительных анкетирований.

Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Проверяйте вложения, полученные по электронной почте, с помощью антивирусного ПО. С осторожностью относитесь к сайтам с некорректными сертификатами. Будьте внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами.

- Не переходите по ссылкам на незнакомые ресурсы, особенно если браузер предупреждает о рисках. Игнорируйте ссылки из всплывающих окон, даже если компания или продукт вам знакомы. Не загружайте файлы с подозрительных веб-ресурсов.

- Заведите отдельную карту для оплаты товаров в Интернете и подключите оповещения по операциям на счете карты.

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА

«ОНЛАЙН ПОКУПКИ»
Якобы продавец просит за товар предоплату либо полную оплату покупки, после чего связь с мошенником прекращается

«МЫ НАШЛИ ВАШИ ДОКУМЕНТЫ»
Якобы нашли ваши утерянные документы и просят вознаграждение за их возврат

«ПРИВЯЗКА КАРТЫ»
Просят привязать вашу банковскую карту к какому-либо номеру телефона или счету

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВЫПЛАТА ПРОЦЕНТОВ»
Обещание больших процентов по вкладам под короткие сроки на различных интернет сайтах

«ПОКУПКА АВИАБИЛЕТОВ»
продажа липовых авиабилетов на мошеннических сайтах

ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ

Помните! Ни в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счету ни под каким предлогом!

Пользуйтесь только проверенными сайтами, на которых решили совершить какие-либо покупки!

Оплачивайте товар только после его получения!

ПОЛИЦИЯ ПОМОЖЕТ 02

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«ВАША КАРТА ЗАБЛОКИРОВАНА»

SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»

Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»

SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»

SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»

Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»

просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Помните! Если вам звонят и тревожным голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники!
Никогда не проходите по ссылкам присланный в SMS-сообщении с незнакомых номеров!
Никому не сообщайте ПИН-код вашей банковской карты!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

Наиболее распространенные схемы онлайн-мошенничества

ВАША УЧЕТНАЯ ЗАПИСЬ БЫЛА ИЛИ БУДЕТ ЗАБЛОКИРОВАНА / ОТКЛЮЧЕНА

Перед угрозой блокировки аккаунта пользователь теряет бдительность, переходит по ссылке в письме и вводит свои логин и пароль.

В ВАШЕЙ УЧЕТНОЙ ЗАПИСИ ОБНАРУЖЕНЫ ПОДОЗРИТЕЛЬНЫЕ ИЛИ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ. ТРЕБУЕТСЯ ОБНОВЛЕНИЕ НАСТРОЕК БЕЗОПАСНОСТИ

В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Пользователь паникует и забывает о бдительности.

Наиболее распространенные схемы онлайн-мошенничества:

ВАШ ДРУГ ОСТАВИЛ ВАМ СООБЩЕНИЕ. ПЕРЕЙДИТЕ ПО ССЫЛКЕ, ЧТОБЫ ПРОЧИТАТЬ

В подобных письмах злоумышленники скрываются за маской людей/организаций, которые входят в ваш доверенный круг, чьи письма и сообщения не должны у вас вызвать подозрений. Люди склонны идти навстречу тем, кому доверяют: переходят по ссылке в письме и вводят свои личные данные.

ПИСЬМА ОТ ГОСУДАРСТВЕННЫХ СЛУЖБ

Фишинговые письма приходят от имени различных госорганов с информацией о претензиях, которые возникли к пользователю со стороны государства. Чаще всего в письмах фигурируют МВД, ФНС и ФМС, а также организации системы здравоохранения.

Наиболее распространенные схемы онлайн-мошенничества

СОЦИАЛЬНАЯ ПОДДЕРЖКА

Благотворительность и меценатство — любимые темы злоумышленников. Чем эмоциональнее обращение к вам, тем больше оснований подозревать мошенничество.
Популярные темы писем: благотворительность после стихийных бедствий, человек в беде, сборы на лечение.

ВЫ ВЫИГРАЛИ

Сообщение о выигрыше и ссылкой на сайт, где якобы можно получить приз.

Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Используйте только лицензионное ПО, регулярно его обновляйте и включайте антивирусную защиту на всех устройствах.

- Важные файлы храните не только на жестком диске компьютера, но и на внешних жестких дисках или в облачном хранилище.

- Используйте двухфакторную аутентификацию, например, для защиты электронной почты. Обязательны сложные пароли из незначащих комбинаций букв, цифр и знаков, не менее 8 символов. Не используйте один и тот же пароль для разных систем. Меняйте пароли хотя бы раз в полгода.