КИМРСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

Памятка «Мошенничество с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации»

декабрь 2024 г.

Мошенничество с использованием информационно-телекоммуникационных технологий в последние годы набирает обороты и уже становится **одним из основных видов**, общей массе зарегистрированных преступлений.

Преступниками постоянно разрабатываются и используются все более ***изощренные способы*** и ***схемы*** хищения денежных средств у граждан.

Актуальные мошеннические **схемы** можно подразделить на несколько **видов**:

Использование личного кабинета «Госуслуги»
Звонящий представляется работником«Госуслуг» или МФЦ и сообщает гражданину, что его личный кабинет пытаются взломать

Мошенник навязывает помощь в смене учетных данных личного кабинета (логина и пароля), для чего владельцу необходимо продиктовать коды, которые ему придут в смс-сообщениях

После получения кодов, мошенник входит в личный кабинет, запрашивает документы, после чего получает возможность получить **онлайн-кредит** на подконтрольную банковскую карту в микро финансовых организациях

Сообщения и звонки на телефон и в мессенджерах
сообщения поступают якобы от сотрудников правоохранительных органов (ФСБ, полиции, прокуратуры и т.д.), с предупреждением потерпевших о попытке хищения денежных средств с банковского счета

Мошенники убеждают потерпевшего перевести денежные средства наякобы ***«безопасный счет»***

После осуществления перевода потерпевший **ЛИШАЕТСЯ ДОСТУПА** к своим деньгам

Важно помнить, чтобы избежать мошенничества, следует быть **ВНИМАТЕЛЬНЫМИ** и **ОСТОРОЖНЫМИ**!

«Фишинг»
Главная цель фишинга состоит в получении конфиденциальных данных пользователей – логинов и паролей

Вводя на сайте данные банковских карт, номера телефона, злоумышленники на основе собранных данных **получают возможность** создать ***дубликат*** банковской карты или ***оплатить товары*** в реальных интернет-магазинах на денежные средства потерпевшего

Признаки отличия поддельных сайтов от настоящих:

Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы ***один символ***
Сайт новый и о нем нет никакой информации в интернете
Тексты на сайте могут содержать ***ошибки*** и ***неработающие ссылки***
Дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка
Вместо названия магазина на аутентификационной странице символы **P2P, PEREVODNAKARTU** или **CARD2CARD**, то есть информация о переводе средств с карты на карту
Сумма на аутентификационной странице банка может быть изменена

Чтобы защитить свои деньги от преступного посягательства **НЕОБХОДИМО:**

- использовать **многофакторную аутентификацию** (отпечаток пальца, голосовые данные пользователя, контрольный вопрос и т.д.)
- использовать сетевой экран с целью **блокирования нежелательного трафика**
- создать **надежный** пароль
- использовать на устройстве актуальную версию **антивирусной программы** с обновленной базой
- не сообщать кому-либо свои персональные данные, **особенно** пароли от личного кабинета, номера и ПИН-коды банковских карт
- **не хранить** такую информацию о личных паролях на компьютере или смартфоне
- перед тем как приобрести товар в интернет-магазине необходимо убедиться, что **адрес сайта является официальным**
- **критично** относиться к сообщениям и звонкам неизвестных, сообщающих о том, что необходимо что-то срочно делать с денежными средствами на банковских счетах

ОТВЕТСТВЕННОСТЬ

1. Ответственность за мошенничество с использованием **электронных средств платежа** предусмотрена ст.159.3 УК РФ

2. Статьей 159.6 УК РФ предусмотрена ответственность за мошенничество **в сфере компьютерной информации**

В случае, если Вы **СТАЛИ ЖЕРТВОЙ** мошенничества – следует **СРОЧНО ОБРАТИТЬСЯ** в правоохранительные органы!