**Прокуратура Павлоградского района разъясняет**

**Новые способы мошенничества с использованием информационно-телекоммуникационных технологий**

В последние годы складывается тенденция к росту количества мошенничеств с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

Учитывая, что мобильные телефоны с доступом к сети «Интернет» имеются у большего числа граждан, в том числе малолетних и пожилого возраста, предполагается, что число мошенничеств в указанной сфере будет только расти. Более того, преступниками постоянно разрабатываются и используются все более изощренные схемы хищения денежных средств у потерпевших.

**1.** **Сообщения и звонки на телефон и в мессенджерах (Telegram, WhatsApp, Viber).**

Данный способ заключается в том, что 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, не давая подумать или проконсультироваться с банковскими работниками, убеждают потерпевшего перевести денежные средства на якобы безопасный счет. После осуществления перевода потерпевший лишается доступа к своим деньгам.

В связи с проводимой специальной военной операцией мошенники стали представляться сотрудниками ФСБ или контрразведки и сообщать потерпевшим, что с их карты осуществляются денежные переводы в поддержку вооруженных сил Украины. За государственную измену лицу грозит длительное лишение свободы с конфискацией имущества, но этого можно избежать, если прямо сейчас перевести денежные средства на специальный счет, контролируемый ФСБ.

**2. Использование личного кабинета «Госуслуги».**

Звонящий представляется работником«Госуслуг» или МФЦ и сообщает потерпевшему, что его личный кабинет пытаются взломать. Мошенник, не давая опомниться, и настаивая, что счет идет на минуты, навязывает помощь в смене учетных данных личного кабинета (логина и пароля), для чего владельцу необходимо продиктовать коды, которые ему придут в смс сообщениях.

Далее после получения от потерпевшего необходимых кодов, мошенник входит в личный кабинет, запрашивает документы, удостоверяющие личность и сведения о доходах владельца (справка по форме 2-НДФЛ), после чего получает возможность получить онлайн-кредит на подконтрольную банковскую карту в микрофинансовых организациях.

**3.** **Фишинг.**

Главная цель фишинга состоит в получении конфиденциальных данных пользователей – логинов и паролей. Мошенники создают поддельные сайты, такие как интернет-магазины, торговые площадки, сайты объявлений и сайты развлекательного контента.

После ввода на таком сайте данных банковской карты и номера телефона злоумышленники на основе собранных данных получают возможность создать дубликат банковской карты или оплатить товары в реальных интернет-магазинах на денежные средства потерпевшего. А полученные аутентификационные данные (логин и пароль) вполне могут подойти для доступа к другим интернет-сервисам и интернет-банкингу.

Чтобы защитить свои денежные средства от преступного посягательства **предлагается следовать нижеперечисленным рекомендациям**:

1) использовать многофакторную аутентификацию. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация (отпечаток пальца, голосовые данные пользователя, контрольный вопрос и т.д.);

2) создать надежный пароль, который должен состоять минимум из 12 символов, содержать заглавные и строчные буквы, специальные символы и цифры. Пароль не должен быть очевидным (например, состоять из последовательных цифр – 12345), не должен содержать запоминающихся комбинаций клавиш на клавиатуре, даты рождения;

3) использовать на устройстве актуальную версию антивирусной программы с обновленной базой;

4) соблюдать осторожность при открытии ссылок, поступивших в электронных сообщениях;

5) не сообщать кому-либо свои персональные данные, особенно пароли от личного кабинета, номера и ПИН коды банковских карт;

6) перед приобретением товара в интернет-магазине убедиться, что адрес сайта является официальным, изучить отзывы интернет пользователей об этом магазине;

7) критично относиться к сообщениям и звонкам неизвестных, сообщающих о необходимости что-то срочно делать с денежными средствами на банковских счетах.

26.01.2024