Киберпреступления и мошенничества

Уважаемые коллеги, киберпреступники осваивают новый способ обмана граждан. Они взламывают аккаунты или создают поддельные учетные записи в социальных сетях и мессенджерах (Whatsapp, Telegram), а также совершают телефонные звонки от имени представителей муниципальных и региональных властей, федеральных структур, клонируют официальные страницы государственных структур. Аккаунты содержат реальные данные (фамилия, имя, отчество, фото и т.п.) и выглядят максимально достоверно. Во всех случаях преступники действуют примерно по сходным сценариям:

1. С поддельных аккаунтов производится рассылка сообщений или звонки с целью получения информации служебного характера. С данных аккаунтов человеку поступает телефонный звонок либо сообщение в социальной сети, мессенджере или по электронной почте якобы от своего руководителя. Злоумышленник обращается к человеку, используя его имя и отчество, чтобы вызвать доверие. В процессе общения злоумышленник предупреждает о последующем телефонном звонке от организации или правоохранительных органов и просит никому о нем не сообщать, а после завершения - отчитаться о результатах разговора. В ходе звонка могут запрашивать различную конфиденциальную информацию и вынуждать совершать противоправные действия в пользу злоумышленников.

Предварительно мошенники собирают информацию о человеке и используют ее в ходе вашего разговора, чтобы вызвать доверие.

2. Мошенники пишут от лица представителей органов власти с просьбой переговорить с так называемым сотрудником ФСБ России (либо МВД или Росфинмониторинга), при этом направляют поддельные приказы о назначении проверки и ответственного за проверку, естественно фамилия проверяющего совпадает с фамилией человека, с которым просят переговорить. При этом мошенники используют искусственный интеллект и нейропсихологическое воздействие. Могут подделывать голос и изображение при видео-звонке.

3. Мошенники, выдавая себя за специалистов различных ведомств и других госструктур, просят у пользователей оказать материальную помощь якобы участникам специальной военной операции.

4. Еще одной из распространенных мошеннических схем является рассылка в социальных сетях и мессенджерах сообщений с предложением проголосовать по различным темам (участие в конкурсе, выбор музыкальной композиции, фильма и т.п.), содержащих ссылку, после перехода по которой легальный аккаунт пользователя перехватывается злоумышленниками. В этом случае необходимо при восстановлении доступа к аккаунту использовать штатные механизмы защиты социальной сети и мессенджера.

Органы правопорядка настоятельно рекомендуют гражданам

быть бдительными. **Представители госструктур или официальные лица не запрашивают в мессенджерах или социальных сетях персональные данные, платёжную и служебную информацию и не просят перевести деньги на банковские карты «для решения проблем», «оказания помощи» или сообщить код из входящего сообщения. Сотрудники ФСБ, МВД и Росфинмониторинга не транслируют в «Telegram» просьбу переговорить, тем более не рассылают ведомственные приказы.**

В качестве примера: мошенники звонят сотрудникам от имени руководителей различного ранга, представляются помощником и далее пытаются получить доступ к служебной информации.

Прошу довести вышеуказанную информацию до сведения государственных гражданских служащих, а также руководителей и сотрудников подведомственных учреждений и профильных организаций.

Обращаем внимание, что необходимо:

1. **Не продолжать диалог, если разговор проходит по одной из указанных выше схем**.
2. В случае повторного звонка – не отвечать.
3. Никому не сообщайте свои персональные данные.
4. Не принимайте необдуманных решений.
5. Всегда относиться с подозрением к неизвестным, которые пишут вам первыми – особенно, если они представляются известной личностью.
6. Если есть сомнения, предложите другой способ связи и сообщите, что вам так удобнее общаться – например, предложите сразу созвониться по видео, или если звонок поступает с мессенджеров, требуйте перезвонить по обычному телефону.
7. Если сообщение поступают с аккаунта знакомого человека – свяжитесь с ним, используя другой способ связи.
8. При поступлении подозрительного звонка или сообщения от якобы руководителя исполнительного органа власти или федеральной структуры свяжитесь с ним самостоятельно, используя доступные средства коммуникации, в т.ч. телефоны, указанные на официальных сайтах исполнительных органов власти и территориальных подразделений федеральных органов исполнительной власти.
9. Не говорите и не вводите пин-код, трехзначный номер или код из СМС.
10. Не набирайте на телефоне никаких комбинаций и не переходите по ссылкам.
11. Не вступайте в длительные разговоры, в случае сомнений прерывайте разговор.
12. Обращайте внимание, если родственник, коллега по работе или знакомый долго разговаривает по телефону – возможно он стал жертвой психологического воздействия злоумышленников.
13. Сделайте скриншоты переписок и аккаунтов и

незамедлительно сообщите о случившемся по единому телефону 112 или телефону 102.