**Профилактика мошенничества**

Чаще всего жертве поступает звонок или сообщение от имени руководителя в нерабочее время с предупреждением, что с жертвой свяжется «куратор от силовиков» или «представитель вышестоящей компании, головного офиса».

➡️ Для правдоподобности используются созданные нейросетями дипфэйки, копирующие голос или изображение, подменные телефонные номера и липовые документы.

➡️ Фэйковый руководитель указывает на большую важность задачи, срочность, абсолютную секретность или большие риски для компании.

➡️ Изучая открытые источники и утечки, мошенник может узнать инсайды компании, что сделает его еще убедительнее.

➡️ Методами социальной инженерии подчиненный вводится в стрессовую ситуацию, лишается способности критически мыслить и отдает мошенникам деньги, платежные средства или важную для организации информацию.

Что делать?

✅Не торопитесь и не паникуйте. Вывести из равновесия – это задача мошенника. Не надо ему помогать.

✅Обратите внимание на адрес, телефон и аккаунт отправителя. Если обычно начальник вам звонит по мобильной связи, а сейчас в мэссенджере – это повод насторожиться.

✅Следите за деталями. Необычное приветствие, обращение или речевые обороты, грамматические ошибки и непривычное оформление документов — все это может быть «красными флагами».

✅Обратите внимание на необычные требования. Если обычно перевод средств согласует шесть человек, а именно сейчас и именно сегодня это требование отменяется, если вам поставлена несвойственная задача, если озвучено требование о секретности – вам звонит мошенник.

✅Свяжитесь с юридическим отделом, службой безопасности или перезвоните руководителю по стандартному каналу связи. Ваше беспокойство о безопасности компании будет оценено.

❗️**ВНИМАНИЕ, РОДИТЕЛИ❗️**

⚠️В соцсетях вирусится (https://iz.ru/1769167/mariia-frolova/do-poslednego-vdokha-v-tiktok-rasprostraniaetsia-smertelnyi-trend-dlia-podrostkov) новый опасный тренд «хромирование», ориентированный на детей и подростков.

❕Детей учат вдыхать токсичные пары от обычных бытовых предметов — дезодорантов, маркеров или лаков для ногтей.

👆Волна деструктивного контента может привести к повышению интереса и нормализации восприятия такого поведения. Для подростка, решившего присоединиться, все может закончиться отравлением, в том числе с летальным исходом или серьезными заболеваниям.

👆Токсикоманию по очевидным причинам нельзя предупредить запретами и изъятиями, поэтому будьте внимательными к вашим детям, формируйте критическое мышление и навыки цифровой гигиены.

**🗣Имитация голоса**

▶️Мошенники научились с использованием нейросетей подделывать голоса родных потенциальной жертвы. Таким образом они вынуждают своих жертв совершать переводы денег.

▶️Чтобы вынудить человека сообщить необходимые сведения или совершить денежный перевод, злоумышленники могут выходить на контакт с человеком от имени знакомых, родных или коллег, имитируя их голоса с помощью специальных программ.

▶️Мошенники используют в подобных схемах нарезки из реальных старых голосовых сообщений жертвы. Сначала они получают доступ к аккаунту, затем начинают писать его контактам с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют тем самым голосовым сообщением якобы от лица владельца аккаунта.

❗️При возникновении сомнений необходимо связаться лично со знакомым, от имени которого звонили, и уточнить у него информацию.

**Опасности использования VPN-сервисов**

➡️Киберпреступники на данный момент заинтересованы в постоянном развитии своих схем обмана и втягивании обычных пользователей в свои преступные действия.

➡️В связи с этим, мошенниками в последние годы активно используются различные VPN-сервисы, чтобы вовлечь пользователей из разных стран мира, из России в частности, в так называемые ботнеты.

➡️Для этого злоумышленники предварительно компрометируют пользовательское устройство, после чего его включают в специальную сеть из огромного количества гаджетов, которые в дальнейшем применяются для проведения DDoS-атак, в том числе и против различных российских государственных ресурсов.

➡️Также нельзя на 100% исключить вероятность того, что установленные на пользовательском компьютере или смартфоне программы, которые предоставляют услуги VPN-сервиса, не будут содержать какого-либо вредоносного функционала.

➡️Обычным пользователям достаточно сложно понять, что их устройство стало частью ботнета, и его активно используют злоумышленники.