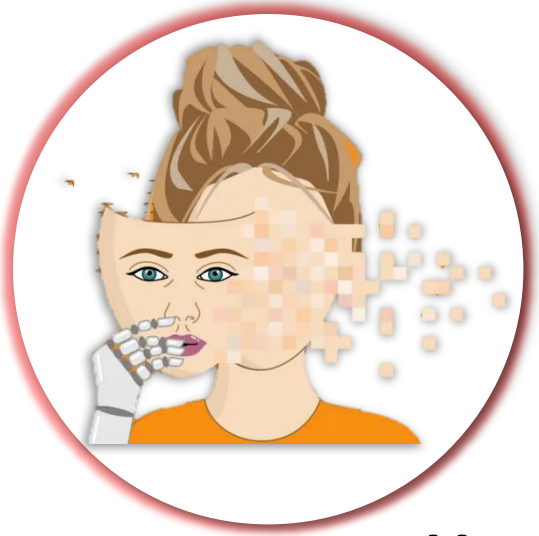
ВИДЫ ФИНАНСОВЫХ КИБЕРМОШЕННИЧЕСТВ

ВИДЫ ФИНАНСОВЫХ КИБЕРМОШЕННИЧЕСТВ

ДРОП

ФИШИНГ

КАРДИНГ



ДИПФЕЙК

Дистанционное мошенничество в отношении граждан

ДРОП

(от английского слова to drop — «бросать») — это подставные лица, которые «прогоняют» по картам похищенные деньги для обналичивания.

Признаки мошенничества

Поиск дропов через объявления о работе (через телеграм-канал/мессенджеры/социальные сети)

- *Объявления составлены с привлекательными критерии*
- *Иногда аферисты не скрывают, что нужно оформить/продать несколько банковских карт.*

Обман с помощью перевода на карту человека. Для этого они похищают данные различными способами:

- *Собеседование с работодателем. Во время собеседования мошенники просят жертву заполнить анкету и указать реквизиты карт, которые оформлены на соискателя.*
- *Фейковые приложения банков. Если человек не увидел подмену, скачал подделку и ввел свои данные, аферисты получают данные его карты.*
- *Социальная инженерия. Это психологические манипуляции с целью заставить человека добровольно сообщить данные своих банковских карт.*

Что предпринять?

Крупные ресурсы — HeadHunter или «Авито» — проверяют работодателей

Использование только официальных приложений банков

Отказ от переводов по неизвестным реквизитам.

Надежное хранение своих банковских реквизитов.

Пользование только проверенными ресурсами в интернете.

Двухфакторная аутентификация для входа в свои учетные записи.

Дистанционное мошенничество
в отношении граждан

ФИШИНГ

переводится с английского как «ловля паролей». В слове phishing совмещаются слова: fishing («рыбалка») и password («пароль»).

Признаки мошенничества

привлекательные сообщения о раздаче денег или «работе с миллионными доходами», на которой ничего не нужно делать. Выманивание паспортных данных, информацию о картах и даже деньги, которые якобы надо внести, чтобы получить гораздо больше.

поддельные сайты, очень похожие на настоящие, изображающие интернет-магазины с заманчиво низкими ценами, альбомы фотографий на облачных сервисах и другие ресурсы, на которых жертва может ввести пароль от важного аккаунта.

Что предпринять?

внимательно проверяйте электронные письма

с подозрением относиться к баннерам — картинка на них может не иметь ничего общего с сайтом, на который вас перекинет

Перед вводом номера карты остановитесь! присмотритесь к адресной строке— опечатки, в неожиданных местах и странные домены. Увидели один из них — покиньте сайт и попробуйте ввести его адрес заново.

Дистанционное мошенничество
в отношении граждан

КАРДИНГ

вид мошенничества, при котором хакеры совершают операцию с использованием платежной карты без участия ее владельца.

Признаки мошенничества

установка скиммера на банкомат (самодельный считыватель магнитной ленты)

кража или незаконное получение карты

«зараженная» точка доступа в общественных местах (считывает информацию с карты)

Что предпринять?

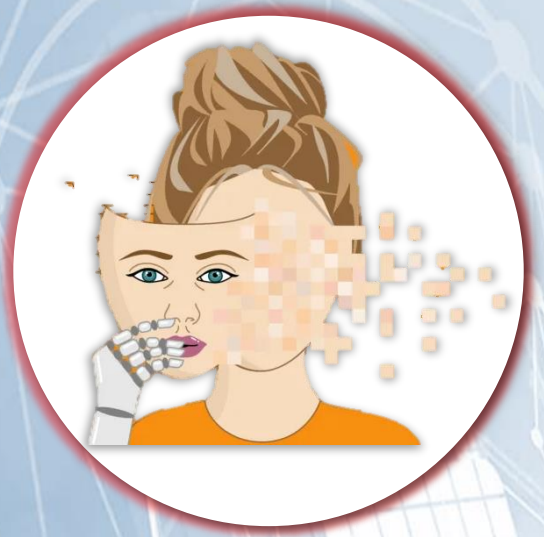
установить многофакторную аутентификацию

обращать внимание на физические признаки взлома банкомата возможно установлен скиммер

установить суточный по лимит по снятию денежных средств

использовать проверенные точки доступа в общественных местах

Дистанционное мошенничество в отношении граждан

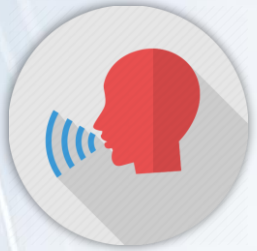


ДИПФЕЙК

(англ. deepfake от deep learning «глубинное обучение» + fake «подделка») — методика синтеза изображения или голоса, основанная на искусственном интеллекте.

Признаки мошенничества

реалистичное видео-изображение человека с помощью нейросети



голос сложно отличимый от голоса прототипа, рассказывающий якобы о своей проблеме и просящий перевести деньги на определенный счет

- дипфейки знакомых
- работодателей
- сотрудников государственных органов
- известных личностей

Что предпринять?

быть разборчивым при получении голосового/ видеосообщения с просьбой о финансовой помощи

не спешите переводить деньги!

обязательно позвоните тому, от чьего имени поступило сообщение, перепроверьте информацию.

Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике.

КИБЕРГИГИЕНА

создавайте надежные пароли

подключите двухфакторную аутентификацию

установите дополнительную защиту в виде пароля или биометрических данных: отпечатка пальца или сканирования лица

будьте внимательны к письмам со ссылками и файлами

будьте внимательны к именам сайтов или отправителям писем

проверьте сайт на безопасность

минимизируйте использование открытого Wi-Fi

УГОЛОВНАЯ ОТВЕТСВЕННОСТЬ ЗА КИБЕРМОШЕННИЧЕСТВО

Ст. 159 УК РФ мошенничество
159.1 - хищения в кредитной сфере
159.2 - хищения социальных выплат
159.3 - хищения с использование электронных платежных средств
159.5 - хищения в страховой сфере
159.6 - хищения в информационно-компьютерной сфере

За данные преступления предусмотрена ответственность — от штрафа до 120 000 ₽ до лишения свободы на 2 года.

Ст. 174-174.1 УК РФ.
Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем

За данные преступления предусмотрена ответственность — от штрафа до 120 000 ₽ до лишения свободы на 5 лет.

Ст. 187 УК РФ (неправомерный оборот средств платежей), согласно которой преступники несут ответственность не только за изготовление и сбыт поддельных банковских карт, но и за разработку и использование технических устройств и компьютерных программ для хищения денег депозитов.

Санкция статьи предусматривает ответственность в виде принудительных работ на срок до 5 лет -лишения свободы до 6 лет со штрафом от 100 000-300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 - 2лет.