ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Если очень просто, то искусственный интеллект (ИИ) — это умная программа, которая может подделывать фото, видео или голос так, что их сложно отличить от настоящих.

Уже совсем скоро, мы будем жить в мире в котором нельзя верить ничему, что мы видим и слышим – всё можно подделать. Уже сейчас мошенники используют современные технологии, чтобы обмануть нас.

Мыслите критически, подвергайте сомнению то, что видите и слышите. А данная памятка поможет вам узнать больше о методах мошенников, использующих технологии для обмана своих жертв.

Поддельные фото в социальных сетях

В социальных сетях профессиональные злоумышленники уже не создают анкеты всего с одной поддельной фотографией. Современные сервисы могут создать десятки вымышленных фото, с одним и тем же человеком. Всё делается для того, чтобы убедить вас, что вы общаетесь с настоящим человеком.

Отныне много фотографий человека – это не показатель, что он действительно существует.

Вымышленные видео

Для посева хаоса и введения в заблуждение, злоумышленники создают новости и подкрепляют их созданными с помощью ИИ видео. Как было в этой «новости» с горящей Эйфелевой башней.

Если вы видите «видео с места событий» — это не значит, что оно настоящее.

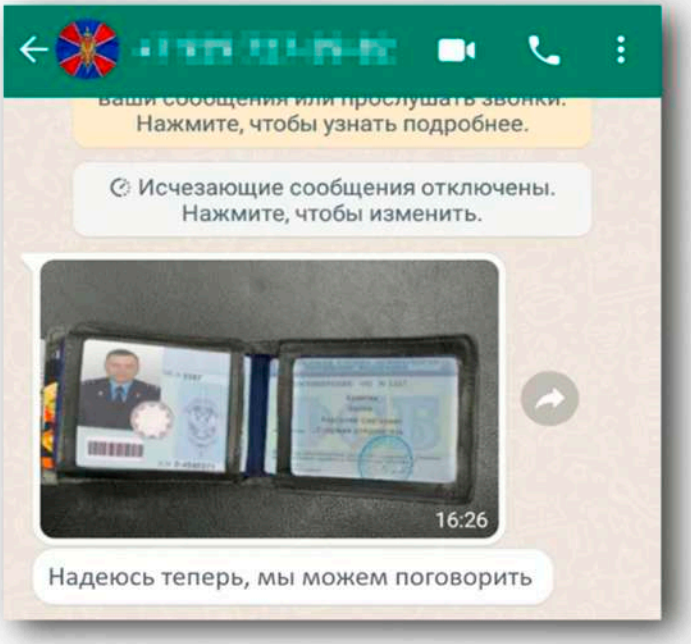
Помимо новостей, вам может встретиться видео, якобы с известным человеком, который будет призывать к чему-то. Даже директор вашей организации может быть подделан и от его имени вам могут сообщить какой-то призыв к действию.

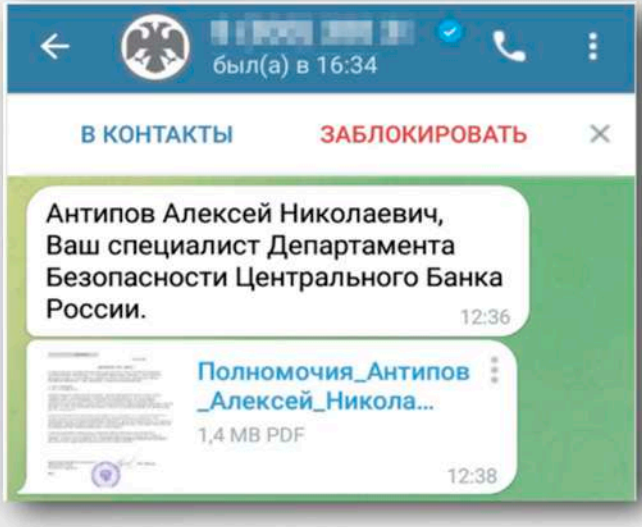
В большей степени можно доверять только официальным каналам связи в вашей организации и даже это стоит перепроверить, если вас призывают сделать что-то необычное.

Поддельные удостоверения

Мошенники для убедительности могут отправить вам свои документы. Такие документы создаются в специальных сервисах или просто используются чужие удостоверения.

Верьте только тем документам, которые вам показывает представитель власти лично (если есть другие доказательства, что это действительно представитель власти).





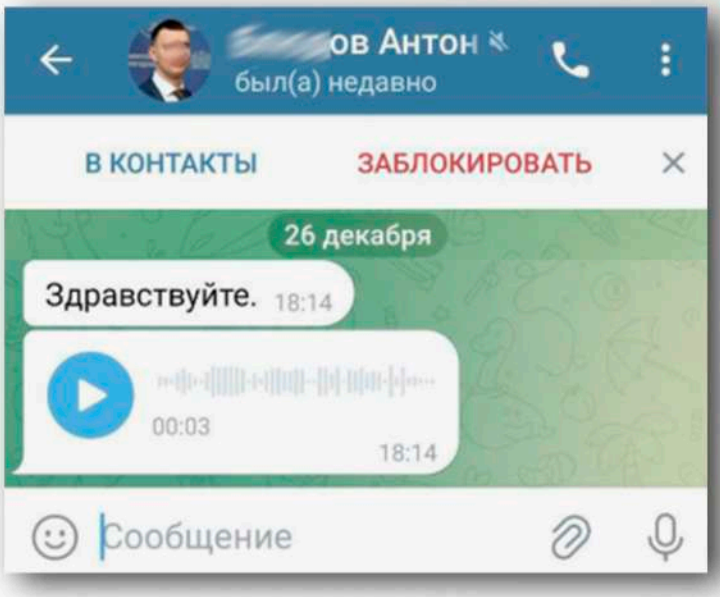
Поддельные документы

В сети существуют сервисы, позволяющие создавать поддельные подписи и печати, имитирующие реальные. Всегда сверяйте эти элементы с официальными образцами.

Строго соблюдайте регламенты документооборота вашей организации. Помните: если документы прислали в мессенджере, например, в Telegram, это не гарантирует их подлинности.

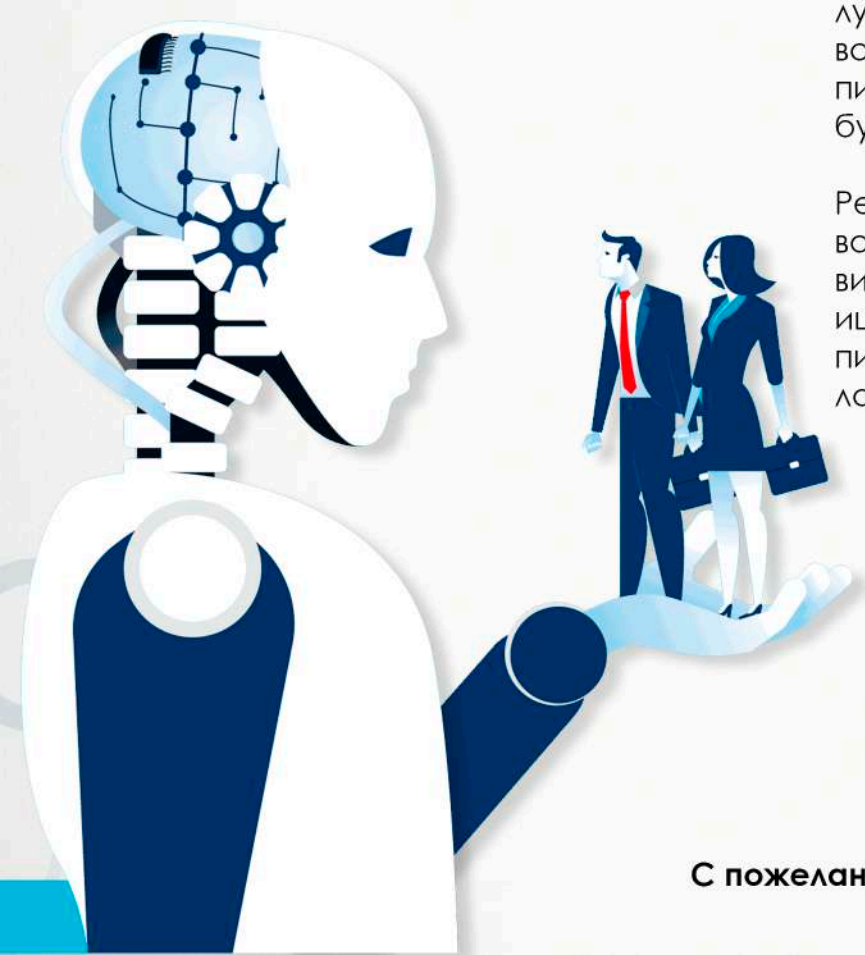
Генерация голоса

Мошенники используют искусственный интеллект для создания голосовых сообщений, похожих на голоса знакомых вам людей и делают это так хорошо, что вы не догадаетесь, что это не ваш знакомый или родственник. Ваш собеседник также может имитировать вашего коллегу или руководителя.



В одной компании были украдены средства после того, как злоумышленники не просто подделали голосовые сообщения, они созванивались с жертвой от имени директора и говорили его голосом.

При получении необычной просьбы в сообщении, лучше перезвоните собеседнику по другому каналу связи или встретьтесь лично. Когда звоните вы, злоумышленник не контролирует все каналы связи и его план проваливается.



Поддельные сообщения

Текстовые сообщения, которые вы получаете по email, также могут создаваться злоумышленниками. Такие письма редко содержат ошибки и будут достаточно убедительными.

Рекомендация тут простая: как только вас просят совершить какое-то действие (открыть ссылку, запустить файл) -- ищите подозрительные признаки в письме и при их нахождении, пересылайте в подразделение ИБ.

С пожеланиями безопасности, StopPhish