Пресс-релиз

«Облако обмана: хранилище, опустошающее кошельки»

Центр прогнозирования преступных угроз и рисков общественной безопасности Комитета по правовой статистике и специальным учетам Генеральной прокуратуры предупреждает о новой схеме интернет-мошенничества, направленной на пользователей облачных сервисов.

По данным зарубежных источников (https://www.theguardian.com/money/2026/apr/12/apple-icloud-storage-scam-emails, https://lenta.ru/news/2026/04/13/apple-scam/, https://www.obozrevatel.com/ekonomika-glavnaya/economy/moshenniki-atakuyut-vladeltsev-iphone-kak-dejstvuet-novaya-shema.htm) злоумышленники массово рассылают пользователям iPhone поддельные электронные письма, SMS-сообщения и уведомления о якобы переполненном облачном хранилище iCloud.

В оповещениях говорится о блокировке аккаунта и возможном удалении фотографий, видео и документов.

Сообщения полностью имитируют официальные уведомления популярных сервисов, включая облачные платформы, что создаёт иллюзию подлинности и подталкивает пользователя к действию.

Для усиления эффекта срочности пользователям предлагают перейти по ссылке и увеличить объём хранилища, обновить платёжные данные или восстановить доступ.

Нажав на ссылку потенциальные жертвы попадают на фишинговый сайт, копирующий оригинальные сервисы, на котором введённые логины, пароли и банковские данные становятся доступны киберпреступникам.

Подобным образом могут рассылаться уведомления о различных сервисах облачного хранения (Google Drive, облако Mail.ru, Яндекс Диск и др.).

Учитывая, что данный вид угрозы начинает распространяться, **рекомендуется**:

- исключить переход по ссылкам из SMS, электронных писем и мессенджеров со «срочными» уведомлениями;

- проверять состояние облачного хранилища только через официальные приложения или сайты;

- не вводить логины, пароли и банковские данные на сторонних страницах;

- включить двухфакторную аутентификацию на всех облачных и почтовых аккаунтах;

- использовать уникальные и сложные пароли для разных сервисов;

- при подозрении на взлом немедленно сменить пароль и завершить все активные сессии.

Сохраняйте бдительность: любые сообщения об удалении данных или блокировки аккаунта проверять только через официальные сервисы.