Cyber Threats

Monthly Cyber Intelligence Summary

December 2024

Mishcon de Reya

It's business. But it's personal.

December 2024 - Cyber Threat Update

Incident	Threat	Key points
Criminals are using generative AI to speed up the process and believability of their fraud schemes.	An FBI alert described the use of AI to generate text, images, audio and video to create convincing lures and artefacts to facilitate fraudulent schemes.	Tips to reduce the risk of falling victim include verifying identities using a codeword, scrutinisng images for tell-tale imperfections, and minimising personal audio and visual content to reduce the risk of impersonation.
Exploitation of Microsoft 365 admin portal for sending sextortion emails	Fraudsters are exploiting the email "Share" option in the Microsoft Admin Portal to send out sextortion emails claiming to have intimate videos and photos of the recipient and demanding ransom.	Raise awareness about the technique with employees. Limit and review access to the Admin Portal to investigate unusual behaviour.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

1. The document has three main purposes to assist cybersecurity leaders:
2. To be 'threat-led' and help prioritise defences against particular types of attackers
3. To justify business decisions on cybersecurity changes, technology or services

To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

FBI warns of use of AI content to facilitate fraud

What happened?

On 03 December, the US Federal Bureau of Investigations (FBI) warned that criminals were exploiting generative Artificial Intelligence (AI) to facilitate fraud on a larger scale.[1] Generative AI speeds up the process and increases the accuracy of believable lures with which to deceive victims, including the use of AI-generated text images, audio and video. This means that fraudsters can "scale up" their campaigns.

Generative AI learns from examples and creates new content from these. Before the use of AI, deceptions could sometimes be detected due to the incorrect use of language, or human errors. Generative AI has made lures more convincing due to the accurate use of language.

Criminals exploit AI-generated text to enhance the credibility of social engineering, spear phishing, romance scams and investments frauds. Criminals are creating social media profiles in bulk and generating believable text for communicating with victims or to populate content on websites such as that in the image below, generated for research purposes. Similarly, AI-powered chatbots are used to get victims to click on malicious links.

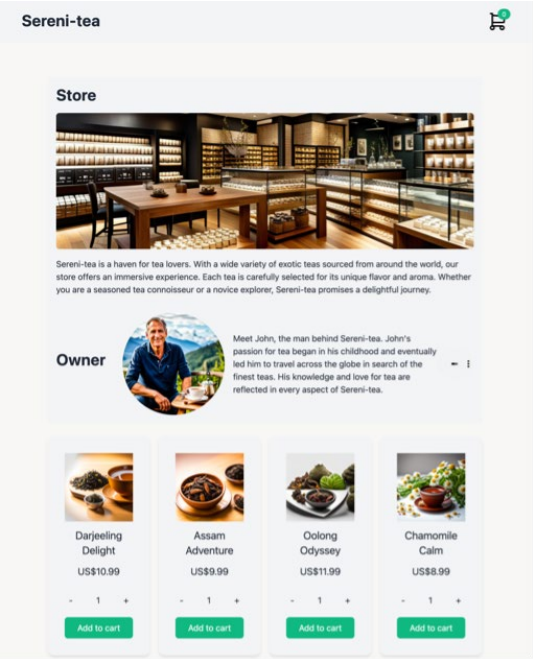

Figure 1 - Example AI-generated website (source: Sophos)

Criminals are also using generative AI to create social media profile images, fraudulent documentation, fake photos, impersonations of celebrities, images of natural disasters to elicit fake charity donations, sextortion images and more.

AI-generated audio, or "vocal cloning" mimics the voices of public figures or personal acquaintances. This can be used to create audio clips that sound like a family member in distress, coercing victims into providing financial aid or meeting ransom demands. It also poses a threat to personal security, as criminals can use these audio clips to impersonate individuals and gain unauthorised access to bank accounts and other sensitive information.

---

[1] Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud, https://www.ic3.gov/PSA/2024/PSA241203

Fraudsters can impersonate company executives, law enforcement, or other authority figures in real-time video chats or to produce evidence that an online contact is a real person. These videos are also used to create promotional materials for fraudulent investment opportunities, adding a layer of legitimacy to their schemes and making it harder for potential victims to discern the truth.

So what?

The outputs of these schemes can be convincing. The FBI have provided a checklist of ways to help identify AI-generated content for use in fraud and extortion. Employees and businesses can use these to help reduce the risks of falling for AI-enhanced scams. Many of the tips rely on increased scrutiny, and a common-sense approach that should be encouraged, regardless of the use of AI, particularly the verification of those that are being interacted with in financial transactions.

Tips include having a secret "codeword" to use with friends and family to verify their identity, scrutinising images and videos for tell-tale signs of manipulation such as distorted body parts, inaccurate shadows, unrealistic movements and unusual lag times.

Where not needed for business development and communications, employees should limit the content of their voices and images online by enhancing social media privacy settings to limit the ability of fraudsters to use this as "training data" for the AI models.

Victims of frauds are encouraged to report to their local police, and through Action Fraud[2] in the UK. If there have been considerable losses as a result, there may be investigative and civil legal routes which can be considered to follow the money and make recoveries. In these instances, it is best to act fast to increase the chances of recovery.

[2] Action Fraud, 6https://www.actionfraud.police.uk/

Exploitation of Microsoft 365 Admin portal for sending sextortion emails

What happened?

On 18th November 2024, it was reported that the Microsoft 365 Admin Portal had been compromised by cybercriminals to send sextortion emails that bypass traditional email security measures. These emails fraudulently claimed that the recipient's computer or mobile device had been compromised to obtain intimate images or videos. The attackers then demanded a ransom, typically between £500 and £5,000, threatening to distribute the content to the victim's contacts.[3]

The scam was executed through the "Message Center" within the Admin Portal, where advisories from Microsoft can be shared with others. Scammers exploited the "Share" feature by entering a "Personal Message" that contained the sextortion note. They circumvented the 1,000-character limit of this field by using browser development tools to increase the maximum length allowed, enabling them to insert lengthy, untruncated messages. These emails are sent from "o365mc@microsoft.com," a legitimate Microsoft address, which lends credibility to the scam and helps it evade spam filters.[4]

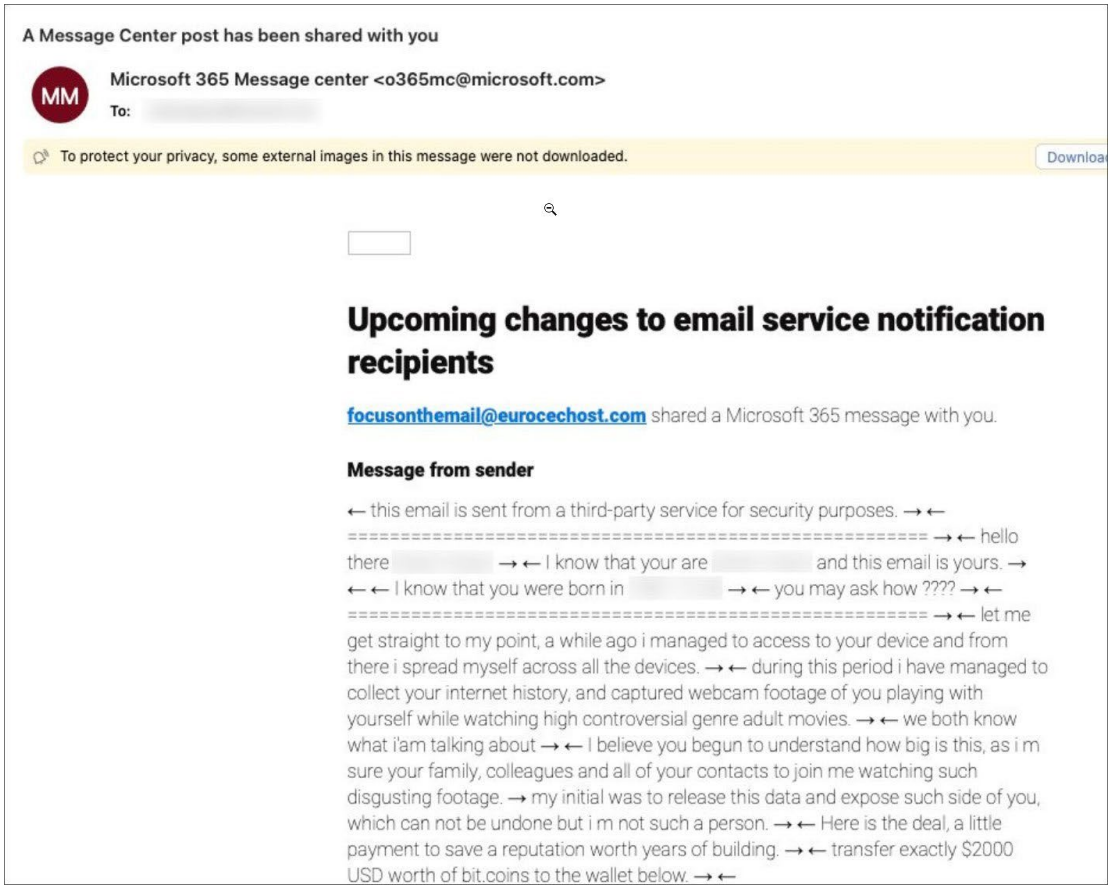

Figure 2 : Sextortion Scam (Source: Bleeping Computer)

[3] Microsoft 365 Admin portal abused to send sextortion emails, https://www.bleepingcomputer.com/news/security/microsoft-365-admin-portal-abused-to-send-sextortion-emails/
[4] I have an email that purports to be from Microsoft 365 Message Centre. It has threatening content. How do I stop the action being threatened? Please see copy of email below. Thanks., https://answers.microsoft.com/en-us/msoffice/forum/all/i-have-an-email-that-purports-to-be-from-microsoft/d8d68580-ee1f-40a6-b022-f74f1794e1ee

So what?

The manipulation of the Microsoft 365 Admin Portal for sending sextortion emails represents another evolution in phishing tactics, one that leverages the trusted reputation of Microsoft to lend authenticity to the attackers' claims. This development is concerning as it suggests a growing adeptness among cybercriminals in exploiting trusted communication channels, thereby increasing the potential for successful extortion.[5]

The use of an official Microsoft email address can deceive recipients into believing the extortion threat is real, potentially leading to financial loss for those who pay the ransom. For individuals unfamiliar with such scams, receiving these emails can cause significant distress and fear. The ability of these emails to bypass security filters undermines trust in existing email security systems.

To counter these threats and enhance protection, businesses can:

- Inform users about this specific scam and general best practices for identifying phishing and extortion attempts.
- Use threat protection services that can detect anomalies in email patterns and content, even if the sender appears legitimate.
- Stay updated with the latest security advisories from Microsoft and promptly apply recommended changes to security settings.
- Promote a culture of security where users are encouraged to report suspicious emails to the IT security team.
- Limit the number of users with access to the Microsoft 365 Admin Portal and monitor activity for unusual behaviour.

In addition to these measures, organisations should reassess their cyber resilience strategies to ensure they are equipped to respond to such threats. This includes regular training for staff, implementing robust access controls, and establishing clear protocols or "playbooks" for responding to security incidents.

Following the reports of these scams, Microsoft has investigated the issue and implemented changes to prevent the misuse of the Message Center for phishing attacks. Now, the "Share" link triggers the user's email client to create a new message, rather than sending it through the portal, which adds an extra layer of scrutiny before an email is sent. Users should continue to be cautious and verify the authenticity of any unexpected or suspicious emails demanding payment or personal information.

[5] Admin Portal Microsoft 365 abused for sending sextortion messages, https://www.techzine.eu/news/security/126329/admin-portal-microsoft-365-abused-for-sending-sextortion-messages/

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com/cyber-risk-and-complex-investigations

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.