Cybersecurity Awareness For Leadership: The Threat of Tycoon2FA

CYBER ALBERTA

Objective

This presentation is a guide to empower leaders across all sectors to recognize and respond to phishing threats. It provides practical guidance to enhance your organization’s cybersecurity posture and protect sensitive information.

What Do We Know About Tycoon2FA

- Tycoon2FA is a user-friendly platform that enables cybercriminals to conduct large-scale phishing attacks without needing advanced technical skills.
- Tycoon2FA streamlines phishing attacks by supplying cybercriminals with pre-configured templates and deceptive web pages that harvest credentials and circumvent two-factor authentication.
- Key features include fake voicemail alerts, document sharing links, and security prompts designed to appear trustworthy and convincing, making it easier to trick people into clicking.

Tycoon2FA And The Rising Threat To Leadership

In light of the recent Tycoon2FA phishing attacks, it’s crucial to raise awareness about the growing risks facing organizational leaders.

Leaders: High–Value Targets

From An Attacker's Perspective, Leaders Are High-Value Targets Because They:

- Have access to sensitive information and critical business practices.
- Have access privileges that are often higher than those of non-executive employees.
- They frequently possess access codes and passwords to the organization's financial data.
- Due to their busy schedules, may inadvertently click on malicious links or provide information without noticing irregularities in targeted communications.

Classification: Protected A

Just The Facts

- According to a recent survey, **96%** of executives failed to distinguish between a real email and a phishing email 100% of the time.
- 65% of Canadian senior executives have been the target of at least one cyberattack in the last 18 months.
- 52% of leaders fear Generative AI may cause major cyberattacks within a year.

Key Statistics On Tycoon 2FA

- In early 2025, Tycoon 2FA accounted for **89%** of phishing-as-a-service incidents, making it the most prominent platform in this category.
- As of 2025, Tycoon 2FA was responsible for **40%** of account takeovers.
- Between August 2023 and February 2024, over **1,200** domains were identified as associated with Tycoon 2FA.

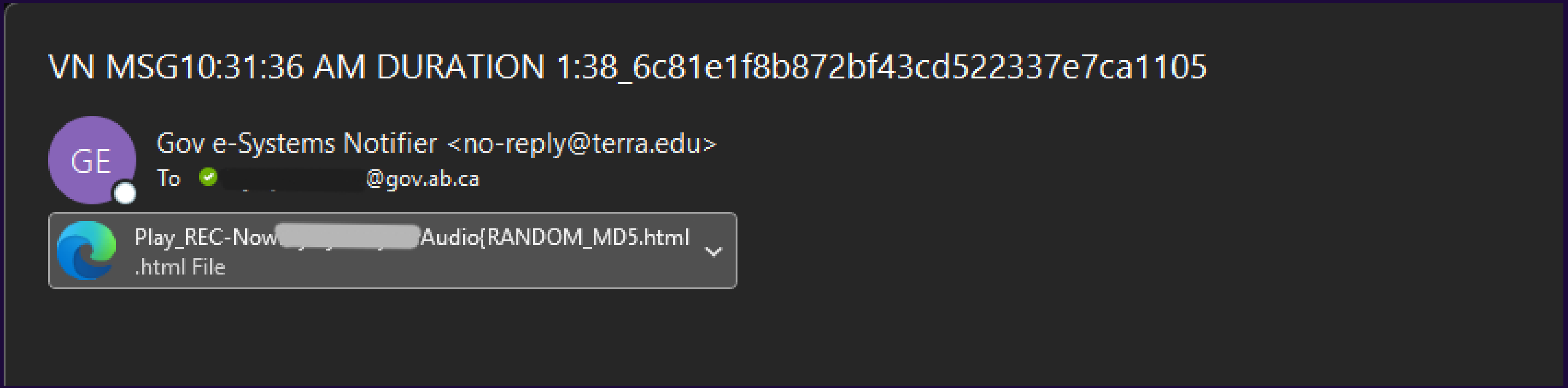
How To Spot Tycoon2FA Phishing Emails

Protecting Leadership From Phishing Attacks

Recognizing A Tycoon2FA Phishing Email

What does this phishing email look like?

- Here is an example:



VN MSG10:31:36 AM DURATION 1:38_6c81e1f8b872bf43cd522337e7ca1105

Gov e-Systems Notifier <no-reply@terra.edu>

To [redacted]@gov.ab.ca

Play_REC-Now[redacted]Audio{RANDOM_MD5.html

.html File

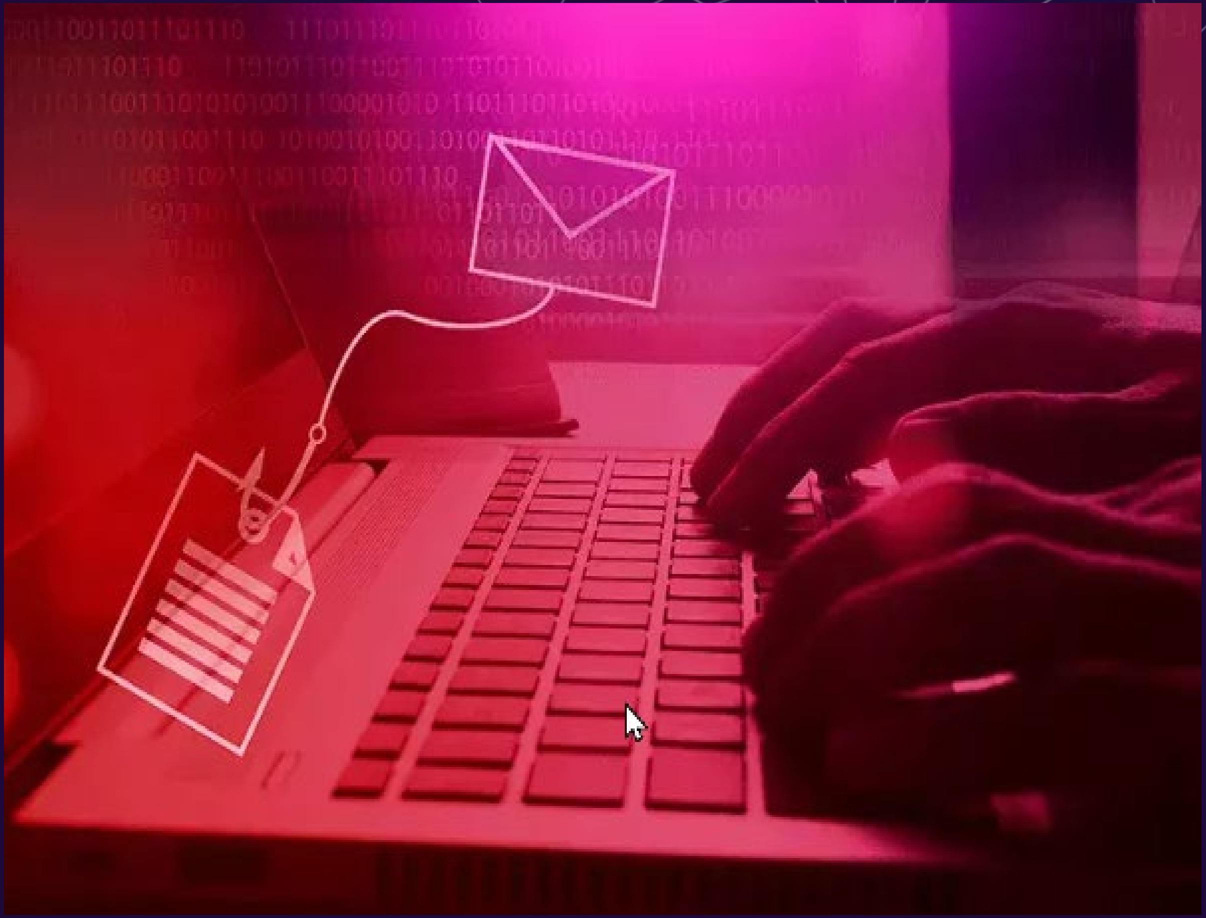
‼️ The primary impact of Tycoon2FA-related activity is credential theft and two-factor authentication (2FA) **bypass.**

What To Watch For

Recognizing Tycoon2FA Phishing Emails:

- The sender appears to be from a legitimate organization.
- There is **no content** in the email body.
- There will be an attachment that includes recipients name in the file name.
- Clicking the attachment leads to a webpage **asking for your login information.**
- Unexpected emails or requests from executives or board members.

Advanced Phishing Techniques



Phishing kits designed to look like real apps and companies that you trust.

Fake websites that block security programs.

Ability to obtain your passwords and login credentials, even while using two steps authentication.

Scanning QR codes, can lead to fake websites.

Best Practices

Recommendations For Leadership To Stay Safe

How To Respond To A Suspicious Email

- Avoid clicking on attachments or links in suspicious emails.
- Never enter your credentials on a webpage accessed through an email link.
- Report the email using your email client's phishing reporting feature.
- If you have clicked on a malicious attachment, immediately contact your IT support team and change your password.
- Take time to slow down and look at where this email is coming from. Check sender address for accuracy.

Additional Suggestions

- Stay Informed: Regularly participate in cybersecurity training and stay updated on the latest phishing tactics.
- Exercise Caution: Scrutinize all emails, especially those from external sources, and treat links and attachments with care.
- Keep sensitive documents off public sites and limit access to executive information. Make it hard for criminals to locate leaders contact information.
- Promote Awareness: Encourage your team to be vigilant and report suspicious emails.
- Implement Security Measures: Ensure you use multi-factor authentication (MFA).

Closing Message

Understanding the specific threats posed by Tycoon2FA and implementing proactive measures is essential for leadership to protect themselves and their organization from phishing attacks. By staying vigilant and prioritizing cybersecurity, you can safeguard your sensitive information and ensure the resilience of your organization.

Together, we can build a safer digital environment. Thank you for your commitment to cybersecurity. **Stay safe!**

Learn More

- ○ Cybersecurity Awareness for Executives
- ○ Advice for Identifying and Responding to Email Phishing Attacks

For a copy of the PowerPoint presentation, please contact
cyberalberta@gov.ab.ca CyberAlberta