Something Seems Phishy

October 7, 2024

TLP: CLEAR

Learn How to Spot Signs of Phishing, Especially from Generative AI

October is observed globally as Cybersecurity Awareness Month, emphasizing the critical importance of cybersecurity in our digital lives. Understanding emerging cyber risks is essential to ensure our online activities — both at work and at home — remain secure.

Throughout October, CyberAlberta provide valuable insights to help us safeguard our digital environments against cyberattacks.

🔍 Identifying Phishing Emails Using Generative AI 🔍

As **Generative AI (GenAI)** gains popularity, phishing emails are becoming increasingly sophisticated to detect. Traditional warning signs are often obscured, making it more challenging to identify fraudulent messages.

🛡️ Tips to Spot a GenAI-Based Phishing Emails 🛡️

Here are key indictors to help you identify potential phishing attempts:

- **Enhanced Legitimacy:** Phishing emails may use polished themes or formatting and display impeccable grammar. However, AI-generated content can occasionally produce awkward phrasing or repetitive sentences, which may seem out of place in typical human communication.
- **Personalization:** These emails may address you personally, sometimes referencing individuals such as your manager or CEO. Be cautious, as they may also appear generic.
- **Contextual Awareness:** Phishing emails often lack specific references to past interactions. Authentic messages typically include details from prior conversations or recent transactions.
- **Visual Elements:** Scrutinize logos and graphics for quality. AI-generated content may struggle to accurately replicate official branding, leading to inconsistencies.
- **Tone of Communication:** Be alert for emails that come across as overly formal or stilted. The tone should align with the usual communication style of the sender.
- **Requests for Sensitive Information:** Be wary of emails asking you to confirm passwords or other personal data.
- **Urgent Language:** Phishing attempts often create a sense of urgency, with threats of account closure or other dire consequences to prompt immediate action.
- **Suspicious Links:** Always verify links and email addresses. Look for subtle errors, such as misspelling in domain names and email addresses (e.g., “Albert.ca**”** instead of “Alberta.ca**”,** **‘teams@**microsfot.com” instead of ‘teams@microsoft.com”).

Phishing emails are becoming harder to detect, especially as cybercriminals use AI to enhance their deception. Staying vigilant and using the tips provided can help protect your personal and organizational information, but always be mindful—think twice before you click.

Traditional Phishing Tactics vs. AI-Generated Phishing Tactics

Aspect	Traditional Phishing	AI-Generated Phishing
Grammar & Spelling	Frequent errors; poorly written	Flawless grammar and spelling
Personalization	Generic greetings (e.g., “Dear User”)	Highly personalized, utilizing public data
Tone	Often awkward or impersonal	Professional and formal, mimics real communication styles
Branding/Visuals	Poor quality logos or mismatched branding	High-quality branding, closely resembling real companies
Contextual Awareness	Irrelevant or vague; lacks details	May include relevant details but often contains subtle errors
Suspicious Links	Obvious, often misspelled domains	More sophisticated, harder to detect
Errors	Easily spotted due to spelling and formatting	More difficult to detect; subtle contextual errors

By remaining vigilant and applying these tips, you can better protect both your personal and organizational information from cyber threats. Always remember to think critically before clicking on any links.

For more information, please visit Cybersecurity awareness and training area of CyberAlberta.