Beware the Phish with Perfect Grammar

cyber security artificial intelligence phishing

Summary: Professional-looking scam emails crafted with AI are now hitting worker inboxes. Unfortunately, their polished look is making it harder to detect fraud. We provide tips for how to spot an AI-generated phishing email.

The browser extension and standalone app, Grammarly, was originally founded in 2009 to help students clean up the grammar in their writing assignments. In the 14Ys since, Grammarly has introduced a tone detector to help writers check how their writing might be perceived, launched Grammarly Business to help companies create style guides and provide writing suggestions, and utilized natural language learning to improve suggestions. Grammarly has 30MM active users.

By contrast, ChatGPT was released for public use in November of 2022. In its first two months, ChatGPT had 100MM monthly users. Unfortunately, some of those users have been scammers, and they're using the technology to craft the perfect phishing emails. This new trend poses a threat to financial institutions, as the new brand of phishing email sounds more professional and plausible than ever. It will take a keen eye and training on what to look for to avoid your institution falling victim.

The Sophistication of Phishing

Artificial intelligence (AI) is smarter than most scammers when it comes to basic grammar, punctuation, and sentence structure. Generative AI like ChatGPT can rid text of the quirky wording, formatting, and misspellings that often characterized phishing emails of the past. Now, AI can produce phishing emails with clean and efficient wording that read like legitimate emails.

This new AI twist makes it even harder for financial institution employees to spot the fakes and resist the temptation to click and fall prey. A mistake can be very costly, as it can trigger a computer kidnapping and ransomware demand. The median amount stolen is now $50K, but losses in the millions are not uncommon.

To make matters worse, Verizon said in its 2023 report on data breaches that fraudulent emails are at an all-time high, and are becoming increasingly sophisticated.

In addition to using ChatGPT to improve their emails, some fraudsters have also employed methods to disguise phishing emails from a distant source into ones that were locally generated, thus making it even harder for threat detection systems to spot, according to Microsoft. Bottom line: an email that appears to come from a boss or a coworker might be a scam.

On top of cyber crooks using the same fake email scams, their tools and methods have gained new sophistication. One recent report by Fortra noted that threats via company inboxes have hit new highs, especially with Phishing-as-a-Service (PhaaS) platforms gaining popularity among cybercriminals. These platforms allow cybercriminals to create high-quality fake pages that they can link to in phishing emails. PhaaS platforms use features like customizing the target victim's link to prefill their company info, logo, and email. The fake pages, which often replicate the look and branding of popular websites and applications, like Microsoft, end up looking quite convincing. This can lead victims to provide passwords and other sensitive

information to what seems like a legitimate site. Nearly all rising cyber scams have used some form of impersonation to trick employees into clicking and providing sensitive information.

Up to now, companies have responded by training employees to avoid emails from unknown sources and to watch for telltale signs of fakery, such as odd wording or spelling. Now that the tools for scamming have grown more advanced, so too does cybersecurity training for employees.

Avoiding the Phishing Hook

Even if your community financial institution (CFI) bolstered its email phishing defenses in the recent past, it's time to reexamine and upgrade threat detection and response. Phishing attempts using AI and location masking are smarter than what financial institutions have gotten used to, and telling employees to look for typos or bad grammar just won't cut it anymore.

CFIs can respond to this new threat by upgrading employee training tactics on phishing scams, and incorporating the following tips for how to spot AI-created phishing emails:

- **Check the sender's email address.** Look closely at the email address and the domain for inconsistent or misleading variations that, at first glance, may make you think it's coming from a trusted source.
- **Examine the URL without clicking on it.** Hover over hyperlinks in the email and look for strange or misspelled domain names that you don't recognize, along with shortened URLs meant to disguise the true link.
- **Look out for generic greetings.** Even with ChatGPT's sophistication, phishing emails may still not use your name, and refer to you as "dear user" or "dear customer." With most email lists requiring you to provide your name to subscribe, an email with a generic greeting has a better chance of not being legitimate.
- **Be wary of urgency.** Phishing emails may use urgent, alarming language to make you panic and click on a link or reply.
- **Verify with the source.** If you're not sure of the legitimacy of the email, contact the sender through another communication method to verify the contents.

Phishing scams using fake emails remain a top security concern for CFIs, and AI has bolstered the ability of fraudsters to make their attempts look real. CFIs need to reevaluate how they train employees to spot phishing emails and look toward upgrading defenses against these sophisticated new hacks.

LOOKING FOR CASH MANAGEMENT SERVICES?

With efficient, cost-effective cash management services, why look anywhere else? PCBB offers ACH, domestic payments, settlement, and overnight sweep to ensure the highest return on your balances. Learn more about our cash management suite today.

ECONOMY & RATES

Rates As Of: 08/23/2023 05:37AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.57	0.02	1.15
6M	5.57	0.04	0.81
1Y	5.36	0.00	0.66
2Y	4.99	0.11	0.56

5Y	4.44	0.26	0.44
10Y	4.28	0.32	0.40
30Y	4.36	0.35	0.40

FF Market	**FF Disc**	**IORB**
5.33	5.50	5.40

SOFR	**Prime**	**OBFR**
5.30	8.50	5.31