Theia Institute℠ Strategic Action Plan

AI-Assisted Phishing

Executive Summary

Focus Question

How should companies address routine phishing attacks[1] enhanced by generative AI systems like ChatGPT?

Key Recommendation

Defend against routine AI-assisted phishing with existing industry-standard tools and best practices.

Strategic Plan

Strategic Assessment

AI tools like ChatGPT, Google's Bard, and BingAI from Microsoft might make phishing emails more convincing, but they don't change the fundamentals of how phishing attacks work. Existing security tools and best practices can effectively protect against AI-assisted phishing threats.

Action Items

1. Implement data loss prevention (DLP) tools to protect sensitive information from being exposed through emails or web connections.
2. Use basic security rules like "separation of duties" and "least privilege access" to protect sensitive data and make it harder for phishing attacks to succeed.
3. Utilize hardware-based multi-factor authentication to increase account security.
4. Integrate biometrics, such as fingerprint or facial recognition, to further secure user credentials.
5. Regularly update and reinforce training to identify and report phishing, adapting to evolving methods and shifting best practices.

Additional Context and Informational Materials

To support the institute's mission and promote transparency, the recommendations have been enriched by podcasts, recorded round table discussions, and other materials provided by our panelists. Please see the following links for more information.

1. An index of available files all in one place online.
2. Copies of this document in PDF format.
3. Video of the round table discussion on YouTube.
4. Audio podcast of the discussion on PodBean.
5. Theia institute's Mastodon account on InfoSec.Exchange.
6. The Theia Institute Community Discussions group on LinkedIn.

[1] Here, "routine phishing attacks" are defined as bulk email-based attacks. Spear-phishing is a more specialized form of social engineering, and will be discussed separately in the future.

About the Theia Institute℠

Theia in Marble, Radiating Light℠

Mission Statement

The growing intersection of data, privacy, and technology requires new ways of thinking about security and how it impacts both business and society. The institute's mission is to provide cutting-edge thought leadership that reframes traditional security leadership for the 21st century by addressing traditional cybersecurity, risk management, and other related topics. In addition, the institute is also tasked with providing practical security solutions within a modern business context.

Consensus-Based Solutions

The institute provides consensus-based recommendations and action items. Each consensus is reached through discussion and debate among the panel's cross-functional members.[2]

[2] The panelists' consensus does not represent an endorsement by any institution or employer other than the panel itself.

The members of the institute collectively believe that truly transformative leadership requires transparency and visibility into core processes. To promote those values and enrich materials the institute makes publicly available, panel discussions and deliberations are available in a variety of formats on multiple social media channels.

Panelists

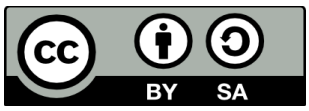
In alphabetical order, the institute's current panelists are:

- Billings, Q. Wade
- Desmond, Jim
- Engel, Barak
- Jacobs, Todd A.
- Palmer, Lisa
- Shannon, Doug

Each panelist brings a unique perspective to the topic. Learn more about their views and perspectives by following the panel's discussions on social media.

Citing and Re-Using Theia Institute[SM] Material

License



Required Attributions

Press Information

For further information about the institute's mission, panelists, or recommendations, please contact our public relations team at press@codegnome.com. We are always glad to provide quotes, background, speakers, and other content to journalists and media outlets.