**2025 CAM EMAIL 1 — Survival Guide Phishing — COPY**

*Subject Line:*

Cybersecurity Awareness Month: Avoid AI-Enhanced Phishing

*Preview Text:*

We’re here to help you overcome the obstacles of AI-enhanced social engineering attacks and stay safe online.

----NEXT SECTION----

*H1:*

**Cybersecurity Awareness Month:**

Avoid AI-Enhanced Phishing

*Subhead:*

Find a Path Past the Hazards of Advance Social Engineering Attacks

*Copy:*

Many sophisticated cyber attacks begin with the same tactic – social engineering. Human risk is prevalent, especially as organizations expand their attack surface (cloud, IoT, hybrid work, etc.), making employees a tempting social engineering target for threat actors looking for access, data, or funds. One of the prevalent — and pernicious — forms is phishing.

**What Is AI-Enhanced Phishing?**
Phishing is a constant threat for organizations, as luring credentials away from employees can give threat actors easy access to your environment and allow them to launch sophisticated attacks. However, it’s become even more dangerous with the rise of AI.

This social engineering standby is evolving, with artificial intelligence helping threat actors avoid telltale signs like spelling and grammatical errors, while also automating time-consuming parts of the attack. If we can no longer rely on poor grammar and composition to tip us off to a phishing attempt, what should we look out for? The answer lies in context. Knowing the types of emails our team and organization sends — and the kinds we’d *never* send. Like:

* A message “from HR” with a company-wide announcement
* A message “from the IT department” asking you to click on a link or provide access to an application
* A message that asks for personal information, such as a date of birth or a Social Security number
* A message that asks for credentials or asks you to authorize a multi-factor authentication (MFA) request

**Other Telltale Signs AI Can’t Avoid**

* The message comes from an unknown sender
* The message employs a sense of urgency or creates an emergency
* The message purports to come from an internal source but uses an external email address or contains external links

We’ll be sharing more about how to overcome the obstacles of AI-enhanced social engineering attacks as the 2025 Cybersecurity Awareness Month continues.

**And, remember, if you ever see something that makes you go ‘hmmmm’, report it to IT right away.**

----NEXT SECTION----

*Footer*