**2025 CAM EMAIL 2 — Survival Guide BEC — COPY**

*Subject Line:*

Cybersecurity Awareness Month: Battle Business Email Compromise

*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:**

Battling Business Email Compromise (BEC)

*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 forms organizations regularly face is BEC attacks, which is now becoming more difficult to battle in the wake of AI enhancements.

**What Is AI-Enhanced BEC?**
In a BEC attack, a hacker gains control of an internal email account and uses that access for financial gain. Traditionally, after gaining access, the bad actor will send out fake emails requesting the transfer of funds, robbing the organization through impersonation.

BEC is a top attack type — and a costly one. Because human risk accounts for 99.2% of root causes of BEC attacks, reducing that risk is paramount to preventing this kind of attack. However, that task is becoming more difficult, as generative AI is helping threat actors spin up fake invoices, create more convincing communication, and conduct needed research for BEC attacks faster and more effectively.

**Find the Path Past BEC Attacks**

* **Be alert to MFA fatigue attacks:** Look out for repeated, uninitiated MFA prompts, which could be a threat actor trying to get you to approve the prompt out of frustration, confusion, or exhaustion.
* **Follow identity and access management (IAM) best practices:** This can prevent credential theft (a root cause of BEC), as well as unauthorized access to important assets or communications that may help a BEC attack succeed.
* **Stay diligent and up to date on security awareness training with BEC simulations:** Our security awareness training utilizes micro-learning, up-to-date information, and simulations of business email compromise can help harden your human attack surface.

More to come next week on the AI-enhanced hazards of social engineering, and how to outfit our organization to overcome them as Cybersecurity Awareness Month continues.

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

----NEXT SECTION----

*Footer*