**2025 CAM EMAIL 3 — Survival Guide Compromised Credentials — COPY**

*Subject Line:*

Cybersecurity Awareness Month: Compromised Credential Crisis

*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:**

The Crisis of Compromised Credentials

*Subhead:*

Find a Path Past the Hazards of Advanced Social Engineering Attacks

*Copy:*

Our friends at Arctic Wolf have informed us that the vast majority of BEC and ransomware cases they have investigated involve stolen or compromised credentials. In addition, it’s been estimated that billions of stolen credentials are available on the dark web — the result of both compromised databases and successful cyber attacks. Be it through phishing, data exfiltration, or successful brute-force attacks, compromised credentials open digital doors for threat actors and lets them wreak havoc on your environment while evading detection. And now, the rise of AI is making obtaining these credentials even easier.

**What Is AI-Enhanced Credential Compromise?**
Credential compromise is the stealing of passwords, usernames, or other data that allows for access to networks, applications, assets, or accounts within an organization’s IT environment. It is used by threat actors looking to launch a cyber attack, move deeper into a system once an attack has begun, complete a financially motivated attack such as business email compromise (BEC), or simply to sell or release on the dark web.

Artificial intelligence technology can automate credential stuffing and brute-force attacks, scan the web to find key data (and potential passwords) of an employee, or quickly decipher the most valuable credentials from a trove of stolen data.

**Let’s Curb Credential Compromise Together**

* **Use multi-factor authentication (MFA), and stay alert to fatigue attacks:** MFA prevents a threat actor from gaining access via compromised credentials, but users should be on the lookout 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.
* **Stay current on security training:** Because credential theft and social engineering tactics like phishing are so interconnected, making sure you're properly informed on how these threats happen can help protect your credentials and reduce human risk.

Even though Cybersecurity Awareness Month is coming to a close, it’s important we keep our culture of security top of mind all year round. We hope you gained valuable insights this Cybersecurity Awareness Month and feel prepared to find the path past AI-enhanced attacks.

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

----NEXT SECTION----

*Footer*