GET THE MOST OUT OF YOUR CYBERSECURITY AWARENESS TOOLKIT

Phishing is the primary method of entry in cyberattacks. These educational materials can help your organization stop phishing and prevent a breach. **Using the kit is simple:**

1. Download the full Cybersecurity Awareness Month (CAM) Toolkit
2. Review all of the included materials, including:
   - CAM overview presentation
   - Three cybersecurity-related infographics
   - Social media tile your team can use to promote CAM on their social channels
   - CAM screensaver you can push to employees
   - CAM email banner your team can add to internal communications throughout the month
3. Upload all the resources to your intranet and add links to the resources hosted on your intranet
4. Share training resources with your internal team and encourage them to register for the Cofense CAM webinars!
5. Deploy your program and engage your workforce to **#BeCyberSmart**
6. Benchmark engagement to report your success!

Follow Cofense on Social Media for the Latest News and Updates on Cybersecurity Awareness Month!

CYBERSECURITY AWARENESS MONTH
OCTOBER 2023

#BeCyberSmart

BUSINESS EMAIL COMPROMISE

is when threat actors use email fraud to attack an organization and its employees, customers or partners.

In the Cofense 2023 **ANNUAL REPORT** we found **10% OF REPORTED** malicious emails were BEC.

TO PROTECT YOUR COMPANY FROM BEC:

- ✓ Use **secondary channels or multi-factor authentication.**
- ✓ Ensure email URLs are **legitimate.**
- ✓ **Do not send login credentials** in response to an email.
- ✓ **Verify** the sender's email address.

OVER THE YEARS, BEC EVOLVED TO INCLUDE:

- ✓ Compromise of personal emails
- ✓ Compromise of vendor emails
- ✓ Spoofed lawyer email accounts
- ✓ Requests for W-2 information
- ✓ Fraudulent requests for large amounts of gift cards

According to the annual **2022 FBI INTERNET CRIME REPORT** BEC phishing cost victims **$2.7 BILLION** this past year alone.

Adopt a **COMPREHENSIVE PHISHING DEFENSE PROGRAM** that empowers all your employees to act as the **first line of defense against BEC scams,** including:

- ✓ A phishing simulation program
- ✓ A reporting tool that allows employees to flag phishing threats

With the rise of BEC, **NO SECURE EMAIL GATEWAY** is **100% EFFECTIVE** in blocking attacks.

RECOGNIZE & REPORT PHISHING
Do Your Part. #BeCyberSmart

COFENSE

LEARN MORE at www.cofense.com

Leverage an Intelligent Email Security solution that brings together crowdsourced intelligence + machine learning to stop attacks.

CYBERSECURITY AWARENESS MONTH
OCTOBER 2023

#BeCyberSmart

CREDENTIAL PHISHING

is when threat actors steal credentials to gain access, bypass an organization's security measures, and steal critical data.

The **2023 COFENSE ANNUAL STATE OF EMAIL SECURITY REPORT** highlighted **CREDENTIAL PHISHING** as the top attack vector with a **478% INCREASE** in malicious emails identified.

CREDENTIALS ARE HIGHLY VALUABLE.

They provide adversaries with access to **sensitive accounts and information** without setting off security alerts.

CREDENTIAL PHISHING PAGES

are inexpensive to host and attackers **can easily change the infrastructure** of these malicious webpages.

CREDENTIAL PHISHING ATTACKS

leave few **indicators of compromise (IOCs),** making breach investigations difficult.

THREAT ACTORS abuse trusted collaboration sites and cloud providers including **Microsoft, Google, Adobe, and DropBox** to deliver credential phishing attacks and malware.

In 2022, **CREDENTIAL PHISHING** was the cyber threat of choice with the average cost of a breach at **$4.5 MILLION.**

RECOGNIZE & REPORT PHISHING

Do Your Part. #BeCyberSmart

COFENSE

LEARN MORE at www.cofense.com

Leverage an Intelligent Email Security solution that brings together crowdsourced intelligence + machine learning to stop attacks.

CYBERSECURITY AWARENESS MONTH
OCTOBER 2023

#BeCyberSmart

RANSOMWARE

is when threat actors steal credentials to gain access, bypass an organization's security measures, and steal critical data.

THE AVERAGE COST of a **ransomware attack** in 2022 was **$4.54 MILLION**

According to the 2022 "Verizon Data Breach Investigations Report," **ransomware** was involved in **25% OF ALL BREACHES.**

IMMEDIATE ACTIONS YOU CAN TAKE NOW TO PROTECT AGAINST RANSOMWARE:

- ✓ Update your operating system and software.
- ✓ Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- ✓ If you use Remote Desktop Protocol (RDP), secure and monitor it.
- ✓ Make an offline backup of your data.

In 2022, the IC3 received **2,385 COMPLAINTS** identified as ransomware with adjusted losses of more than **$34.3 MILLION**

BY 2031, RANSOMWARE WILL COST its victims around **$265 BILLION** annually, with a new attack every **2 SECONDS.**

Even if an organization pays a **ransom settlement**, they only get **60%** of their data back.

Only **4%** get all of their data.

RECOGNIZE & REPORT PHISHING

Do Your Part. #BeCyberSmart

COFENSE

LEARN MORE at www.cofense.com

Leverage an Intelligent Email Security solution that brings together crowdsourced intelligence + machine learning to stop attacks.