U.S. DEPARTMENT OF EDUCATION

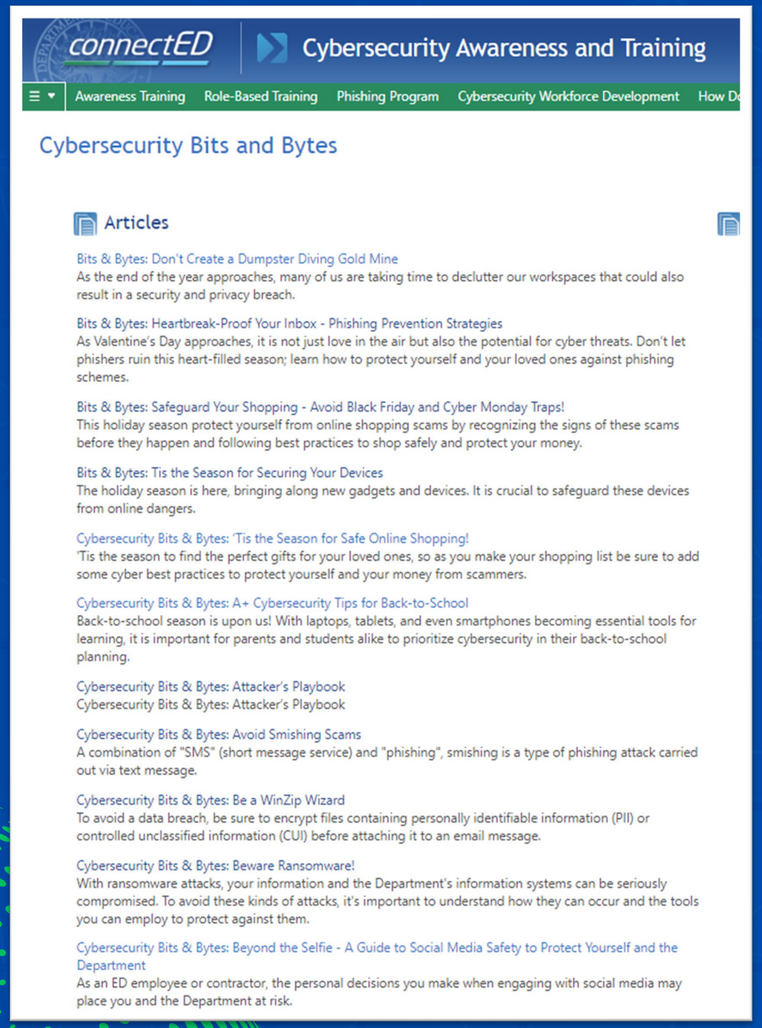
CYBERSECURITY BITS AND BYTES

TAKING ON CYBER AWARENESS ONE BIT AND ONE BYTE AT A TIME

Cybersecurity Blog

In partnership with K2SHARE

A BIT ABOUT THE BITS AND BYTES BLOG



- The goal of the Cybersecurity Bits and Bytes blog is to **spread awareness of current cybersecurity threats and vulnerabilities and to influence reader behaviors based on best practices.**
- The U.S. Department of Education (ED)'s Cybersecurity Bits and Bytes blog features **new cybersecurity awareness content on a bi-weekly basis.**
- A link to each new blog post is **included in ED Notebook, ED's intranet homepage**.

A BYTE MORE ABOUT THE BITS AND BYTES BLOG

- **Catchy titles** and **graphics** are used to draw readers' attention to the awareness content that was **designed to take only 3 to 5 minutes to read.**
- Users may use the blog posts as a **job aid** or include the information and **tips in Principal Office level communications.**
- Each post follows a **specific "recipe,"** so readers are familiar with the format and know where to find specific information.

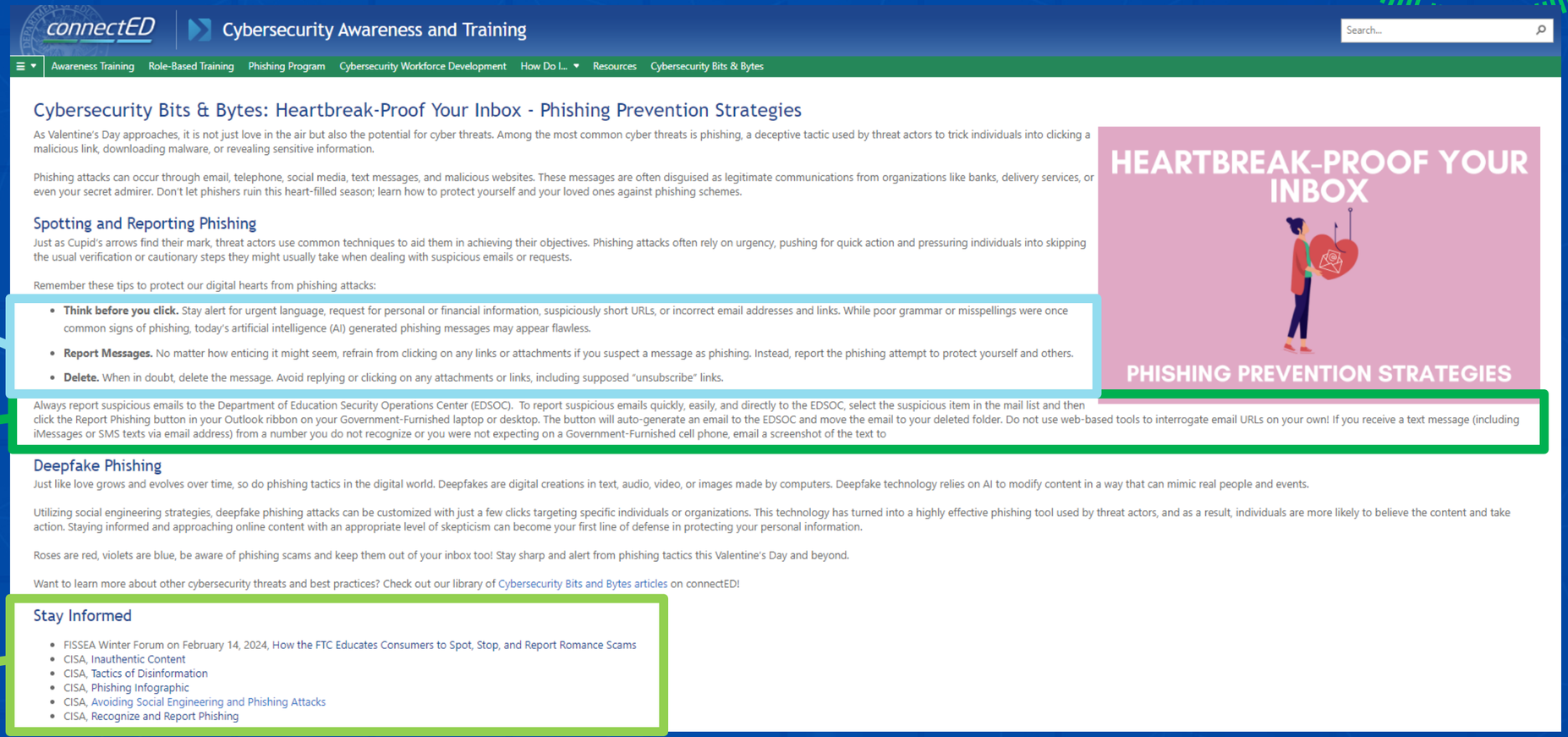
RECIPE FOR CYBERSECURITY BITS AND BYTES

In addition to general information about the featured topic, each Bits and Bytes article includes:

Best practices users can implement at work and at home to reduce risk.

Instructions on how to report known or suspected cybersecurity incidents and phishing attacks.

Links to additional information available on other government sites to enhance learning.



connectED | Cybersecurity Awareness and Training

Search...

Awareness Training | Role-Based Training | Phishing Program | Cybersecurity Workforce Development | How Do I... | Resources | Cybersecurity Bits & Bytes

Cybersecurity Bits & Bytes: Heartbreak-Proof Your Inbox - Phishing Prevention Strategies

As Valentine's Day approaches, it is not just love in the air but also the potential for cyber threats. Among the most common cyber threats is phishing, a deceptive tactic used by threat actors to trick individuals into clicking a malicious link, downloading malware, or revealing sensitive information.

Phishing attacks can occur through email, telephone, social media, text messages, and malicious websites. These messages are often disguised as legitimate communications from organizations like banks, delivery services, or even your secret admirer. Don't let phishers ruin this heart-filled season; learn how to protect yourself and your loved ones against phishing schemes.

Spotting and Reporting Phishing

Just as Cupid's arrows find their mark, threat actors use common techniques to aid them in achieving their objectives. Phishing attacks often rely on urgency, pushing for quick action and pressuring individuals into skipping the usual verification or cautionary steps they might usually take when dealing with suspicious emails or requests.

Remember these tips to protect our digital hearts from phishing attacks:

- **Think before you click.** Stay alert for urgent language, request for personal or financial information, suspiciously short URLs, or incorrect email addresses and links. While poor grammar or misspellings were once common signs of phishing, today's artificial intelligence (AI) generated phishing messages may appear flawless.
- **Report Messages.** No matter how enticing it might seem, refrain from clicking on any links or attachments if you suspect a message as phishing. Instead, report the phishing attempt to protect yourself and others.
- **Delete.** When in doubt, delete the message. Avoid replying or clicking on any attachments or links, including supposed "unsubscribe" links.

Always report suspicious emails to the Department of Education Security Operations Center (EDSOC). To report suspicious emails quickly, easily, and directly to the EDSOC, select the suspicious item in the mail list and then click the Report Phishing button in your Outlook ribbon on your Government-Furnished laptop or desktop. The button will auto-generate an email to the EDSOC and move the email to your deleted folder. Do not use web-based tools to interrogate email URLs on your own! If you receive a text message (including iMessages or SMS texts via email address) from a number you do not recognize or you were not expecting on a Government-Furnished cell phone, email a screenshot of the text to

Deepfake Phishing

Just like love grows and evolves over time, so do phishing tactics in the digital world. Deepfakes are digital creations in text, audio, video, or images made by computers. Deepfake technology relies on AI to modify content in a way that can mimic real people and events.

Utilizing social engineering strategies, deepfake phishing attacks can be customized with just a few clicks targeting specific individuals or organizations. This technology has turned into a highly effective phishing tool used by threat actors, and as a result, individuals are more likely to believe the content and take action. Staying informed and approaching online content with an appropriate level of skepticism can become your first line of defense in protecting your personal information.

Roses are red, violets are blue, be aware of phishing scams and keep them out of your inbox too! Stay sharp and alert from phishing tactics this Valentine's Day and beyond.

Want to learn more about other cybersecurity threats and best practices? Check out our library of Cybersecurity Bits and Bytes articles on connectED!

Stay Informed

- FISSEA Winter Forum on February 14, 2024, How the FTC Educates Consumers to Spot, Stop, and Report Romance Scams
- CISA, Inauthentic Content
- CISA, Tactics of Disinformation
- CISA, Phishing Infographic
- CISA, Avoiding Social Engineering and Phishing Attacks
- CISA, Recognize and Report Phishing

BITS AND BYTES BLOG TOPICS

A selection of Bits and Bytes topics from the previous year include:

- Detecting AI Scams
- A+ Cybersecurity Tips for Back to School
- ‘Tis the Season for Safe Online Shopping
- Beyond the Selfie: A Guide to Social Media Safety
- Heart-break Proof Your Inbox: Phishing Prevention Strategies
- Leveraging Artificial Intelligence Tools Safely
- Mind Games: The Hidden Power of Social Engineering
- Tips for a Secure Tax Season