

### 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

Cybersecurity Awareness and Training

Cybersecurity Bits and Bytes

connectED

#### Articles

#### Bits & Bytes: Don't Create a Dumpster Diving Gold Mine

As the end of the year approaches, many of us are taking time to declutter our workspaces that could also result in a security and privacy breach.

Ξ ▼ | Awareness Training Role-Based Training Phishing Program Cybersecurity Workforce Development How De

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. Don't let phishers ruin this heart-filled season; learn how to protect yourself and your loved ones against phishing schemes.

Bits & Bytes: Safeguard Your Shopping - Avoid Black Friday and Cyber Monday Traps! This holiday season protect yourself from online shopping scams by recognizing the signs of these scams before they happen and following best practices to shop safely and protect your money.

#### Bits & Bytes: Tis the Season for Securing Your Devices

The holiday season is here, bringing along new gadgets and devices. It is crucial to safeguard these devices from online dangers.

Cybersecurity Bits & Bytes: 'Tis the Season for Safe Online Shopping! 'Tis the season to find the perfect gifts for your loved ones, so as you make your shopping list be sure to add some cyber best practices to protect yourself and your money from scammers.

#### Cybersecurity Bits & Bytes: A+ Cybersecurity Tips for Back-to-School

Back-to-school season is upon us! With laptops, tablets, and even smartphones becoming essential tools for learning, it is important for parents and students alike to prioritize cybersecurity in their back-to-school planning.

Cybersecurity Bits & Bytes: Attacker's Playbook Cybersecurity Bits & Bytes: Attacker's Playbook

Cybersecurity Bits & Bytes: Avoid Smishing Scams A combination of "SMS" (short message service) and "phishing", smishing is a type of phishing attack carried out via text message.

#### Cybersecurity Bits & Bytes: Be a WinZip Wizard

To avoid a data breach, be sure to encrypt files containing personally identifiable information (PII) or controlled unclassified information (CUI) before attaching it to an email message.

#### Cybersecurity Bits & Bytes: Beware Ransomware!

With ransomware attacks, your information and the Department's information systems can be seriously compromised. To avoid these kinds of attacks, it's important to understand how they can occur and the tools you can employ to protect against them.

Cybersecurity Bits & Bytes: Beyond the Selfie - A Guide to Social Media Safety to Protect Yourself and the Department

As an ED employee or contractor, the personal decisions you make when engaging with social media may place you and the Department at risk.

• 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. Cybersecurity Bits and Bytes blog features new cybersecurity awareness content on a bi-weekly

• The U.S. Department of Education (ED)'s basis.

 A link to each new blog post is included in ED Notebook, ED's intranet homepage.



### **U.S. Department of Education**

■ K2SHARE

## **A BYTE MORE ABOUT THE BITS AND BYTES BLOG**



All new employees and contractors with significant IT security responsibility must also complete Role-Based Cybersecurity Training.

CSPA Training is an annual requirement. Employees must complete all training in curriculum by posted due date.



#### Articles

Bits & Bytes: Tis the Season for Securing Your Devices

#### Documents

Digital Signatures Job Aid Digital Signatures Job Aid

 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.** 



### U.S. Department of Education

• Each post follows a **specific "recipe**," so readers are familiar with the format and know where to find specific information.

■ K2SHARE

## **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

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

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

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 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, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications from organizations like banks, delivery services, of the services are often disguised as legitimate communications are often disguised a 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"

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 click the Report Phishing button in your Outlook ribbon on your Government-Furnished laptop or desktop. The button will auto-generate an 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. Staving 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



### U.S. Department of Education

HEARTBREAK-PROOF YOU PHISHING PREVENTION STRATEGIES



## **BITS AND BYTES BLOG TOPICS**

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

- Detecting Al 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



#### Cybersecurity Bits & Bytes: 'Tis the Season for Safe Online S

with the hold season upon us and as wings-filled days like Black Findary and Cyber Monday approaching fact, be sure you are protecting your wallet from online shopping scans! Tis the season to find the perfect gifts for your loved nee, so as your make your shopping list be sure to add some other perfect gifts for your loved from commande your shopping list be sure to add some other bractices to protect yourself and your money from scanmers.

#### of Online Shopping Scams

- The Hot Deal Scam or Grinch Bots: Drey holiday season, there are popular products that consumes receil the item for a huge mark-up online. Buying form resile markets is risky and can lead to finaud or behave like leiphome realisers, scammes pretend to sell these hard-to-find products at extremely to payment and shipping information.
- these types of emails to track delivery. • The Fabricated Website Scam: Bad actors will create entire websites meant to scam consumers into legitimate retailer sites with slight spelling variations to the website name. Also be cautious of social m products.

#### ps for Safe Online Shopping

- Always Think Before You Click: Holiday phishing emails can be tricky to spot as they may be designe
- clicking a link or attachment in email or text if you are not sure or the sender closely examine the me Check Your Devices and Accounts: Before you dive into the deals, be sure that the device you are sho before you are shown and the sender of the sender of the sender – closely examine the me of the sender – closely examine the sender – closely examine the me of the sender – closely examine the sender – closely examin
- Pay with a Credit Card, Rather than a Debit Card: If you receive a fraudulent charge, credit transac
  Monitor your Credit and Accounts Closely During the Shopping Season: You should always keep

#### Awareness Training Role-Based Training Phishing Program Cybersecurity Workforce Development How De

#### Cybersecurity Bits & Bytes: Leveraging Artificial Intelligence Tools Safely

Cybersecurity Awareness and Traini

Artificial Intelligence (AI), once a concept from futuristic science-fiction movies, has moved from the big screen into our everyday lives, including the workplace. At consists of software algorithms with the capability to learn and become increasingly better at carrying out specific tasks as they are exposed to more data; it employs techniques from machine learning and deep learning to natural language processing and robotics. At tools like ChatGPT, LumeS, and Bard, among many others can streamline tasks, increase efficiencies, and even foster innovation by creating techniques from machine learning and deep learning to natural language processing and robotics. At tools like ChatGPT, LumeS, and Bard, among many others can streamline tasks, increase efficiencies, and even foster innovation by creating text, music, and visual content for the user. In the world of oyber, AL can even be leveraged for software development and cybersecurity monitoring. However, like any new innovative tool, it is essential to be aware of the risks associated with using AI and the appropriate spaces in which to employ it. In fact, as an employee of the Department, you should be aware of thow using AI in the workplace can present significan cybersecurity threats.

#### What are the Risks of Using Artificial Intelligence

Though the primary goal of AI is to enhance the functions of computer-based learning and perception, the storage of data within the AI platform itself is what can threaten the cybersecurity and privacy of individual users and the Department as a whole. If ED employees or contractors were to share Department information with AI tools to create presentations or finish writing reports by inputting existing ED information, they would inadvertently be allowing unauthorize access and disclosure of that promistary information, some additional increasing noncements hand to loci include:

- Al Hallucination: Al systems can create content that includes information incorrectly or out of context and may even fabricate information complement of the part fabric fabricated by Al an already virtualities on the internet creating daggerous fabric antipartities.
- Al Bias and Misinformation: Machine learning is not always able to differentiate facts from misinformation, nor is it able to understand bias

#### Can I Use AI on My GF

connectED

- partment information should only be processed, publicized, generated, communicated, or stored on devices and services that are authorized by to an antinartment policies and procedures on records management and privacy protections. If you have questions about approved software and hardware
- f you have shared information with ChatGPT. Bard. or any other AI model, you should notify the ED Security Operations Center (EDSOC) at (202) 24

#### litional Resources

- White House Fact Sheet, Biden Harris Administration Announces New Actions to Promote Responsible Al Innovation: https://www.whitehouse americans-rights-and-safety/
   Department of Education Technology Standards and Products Guide: https://usdedeop.sharepoint.com/sites/EnterpriseProgramManagement
- Harvard Business Review, The New Risks ChatGPT Poses to Cybersecurity: https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecu



#### L. • Resources Cybersecurity Bits & Bytes

#### hopping!

can set for online shoppers. Here are a few of the most popular online shopping scams to avoid clicking

sh to buy for loved ones. Automated programs can quickly buy these scarce, highly sought-after holiday items and ther unterfeit goods. It is best to avoid Grinch Bot sales and only buy from vendors you can verify. Bad actors may also ices, which leads shoppers to pay for the product and never necive it or compromise their identity after entering

r jou to their for indexing. As you must receive a nore of packages and season, and actors realize and you in be expected

ia retailers who are selling their products as incredibly low prices, especially if you cannot find extensive re

#### yber safety shopping list should be these best practices:

to look like real retailers. While it may be tempting to click immediate age first for signs of phishing. Be especially suspicious if asked to pay ping on is fully up to date. Also assess all your accounts to ensure they

ped from before. If you are unsure, try to research the retailer before nline shopping or banking.

lose eye on your credit and account transactions, but especially during

bersecurity Bits & Bytes: Mind Games - The Hidden Power of Social Engineering you ever wordered how a seemingly hamless email or social media message could lead to a major security breach in even the most technologically advanced orga

Social engineering utilizes the most unpredictable element of security systems - human psychology. With this in mind, it is essential recognize the signs of social engineering and what to do to guard against scams the

and complete the content by filling it with information the user doesn't have

#### DINNECTED Sybersecurity Awareness and Training

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

#### bersecurity Bits & Bytes: Tips for a Secure Tax Season

as season approaches, many Americans face an increase in scams where imposters pretend to be the Internal Revenue Service (IRS). This results in significant financial losses and at times, even identity theft. These scams often use tricky is to obtain money or entract personal information, which can be used later for filing deceptive tax returns. To protect yourself during tax season, it is essential to understand these common tactics to defend your dollars and keep your and information common

#### Understanding and Recognizing Tax Scam Tactic

ert for tax scam tactics! Stay vigilant against attempts to collect your personal information. Common tactics associated with tax scams include

- Phishing and Smishing. As public awareness of tax scams has increased, threat actors have adapted their strategies. Smishing, a blend of SMS (text messaging) and phishing, is one of the most common forms of communicati used to deceive users. These messages often promise a tax rebate, refund, or other benefits. Stav cautious since these unsolicited messages may encourage you to click on a link or disclose personal and financial information th
- threat actors can use to exploit your money or identity. Vishing: Vishing is a phishing attack where threat actors utilize voice communications to trick individuals into sharing sensitive information over the phone. Besides emails and text messages, threat actors frequently resort to phore lises, clean preteriors the Tisk trib tripical approach involves creating a sense of urgency and insisting that immediate payment is required, often in the forms of gift cards or wire services. Be wary of unsolicited calls

#### v can I protect myself from tax scams

g a clear understanding of how the IRS does (and does not) work is the strongest foundation for protecting yourself. Two key guidelines to kno

The lists with four contact you wap income, enabled, or social means advoct money of web or negative and account of the account of the lists command and have the DC characteria to active any account of the lists command and have the DC characteria to active any account of the lists command and have the DC characteria to active any account of the lists command and have the DC characteria to active any account of the lists command account of the lists command account of the DC characteria to active any account of the lists command account of the DC characteria to account of the lists command account of the DC characteria to account of the lists command account of the DC characteria to a

are also several proactive actions that can be taken to safeguard your personal data:

Following ophesecurity best practices is crucial to avoiding falling for phishing, smishing, or other attacks. This involves exercising caution with links, verifying the identity of senders, and refraining from sharing personal or financial information through phone calls, emails, or text messages. File your tax return promptly, as the IRS only accepts one return per Social Security number, making it more challenging for fraudulent submissions.

Ensure you submit your taxes solely through secure sites and with verticed preparers.

#### tional Resources:

IPC Tay Scome (Consumer Alacte Neuroper) https://www.irc.gov/neuroper.dov.come.com/umor.alacte

- IRS Identity Theft Central: https://www.irs.gov/identity-theft-central
- IRS How to Report Tax Scams: https://www.irs.gov/businesses/small-businesses-self-employed/tax-scams-how-to-report-them

R: If an email is asking you to click a link or submit personal information, always check the sender's name and email address. NEVER follow links in emails that route you outside the ED Network and NEVER give out your personal information. OCIO and its contractors will NEVER ask you for your

#### **DEFEND YOUR DOLLARS**







