Security Awareness Training

Dan Boyle, PERAC IT Director

Norwood, MA
March 3, 2026

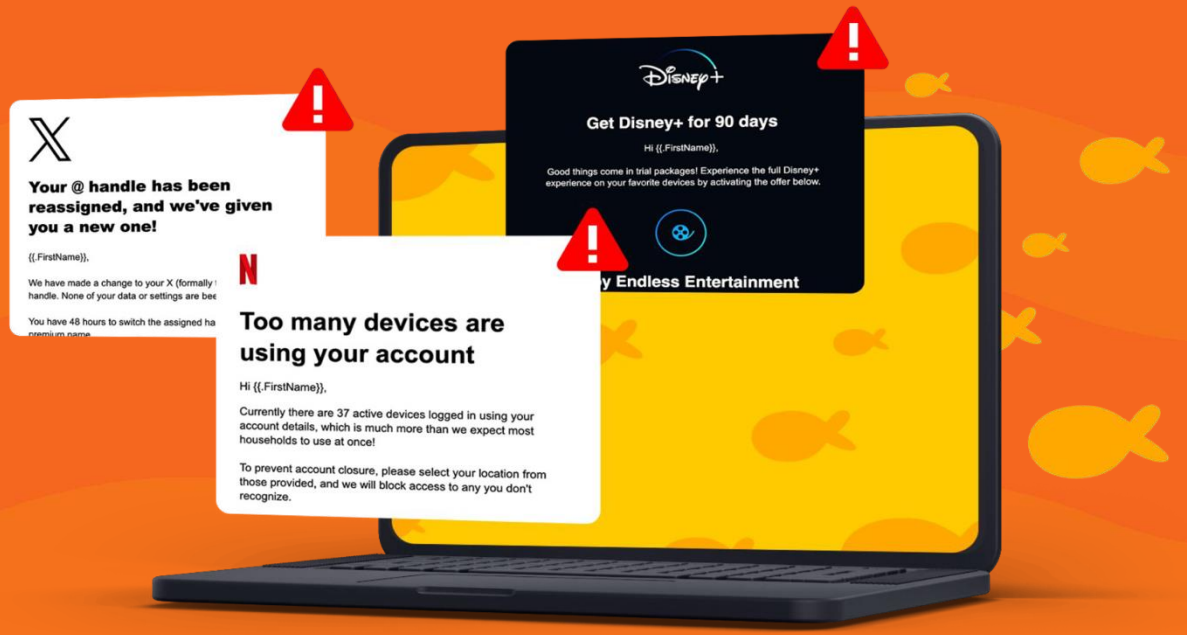
Slides from wizer-training.com

Statistics: Identity Theft and Cybercrime

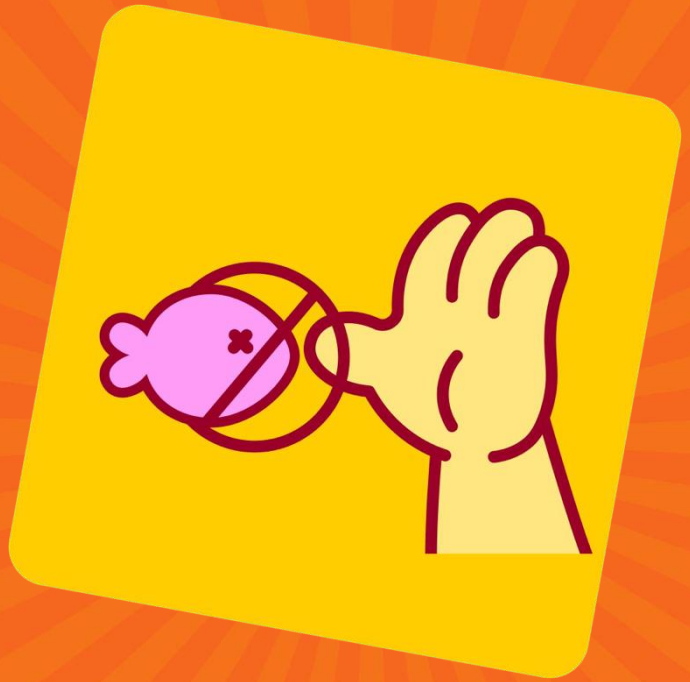
- Practically every American's personally identifiable information — including birthdates, addresses, and Social Security numbers — is available on the dark web, says Bryan Vorndran, head of the FBI's cyber division, and can be purchased for as little as $2
  - Watch Video https://www.youtube.com/shorts/5tNHF7De7yE?feature=share
- According to The Identity Theft Research Center (ITRC) Annual Data Breach Report, 2024 had the second-highest number of data compromises in the U.S. in a single year since the ITRC began tracking data events in 2005, down just one percentage point from the record set in 2023. There was a total of 1.35 trillion victim notices issued including five mega breaches resulting in 100 million to 560 million victim notices issued each, or 83 percent
- The annual global cost of cybercrime is estimated to reach $10.5 trillion dollars in 2025, according to Cybercrime Magazine. Yet, the rate of prosecution for cybercrimes is as low as 0.05%, according to the World Economic Forum's The Global Risks Report 2020.

Phishing

When scammers **FOOL YOU** to think they are someone you trust in order to make you **DO SOMETHING**

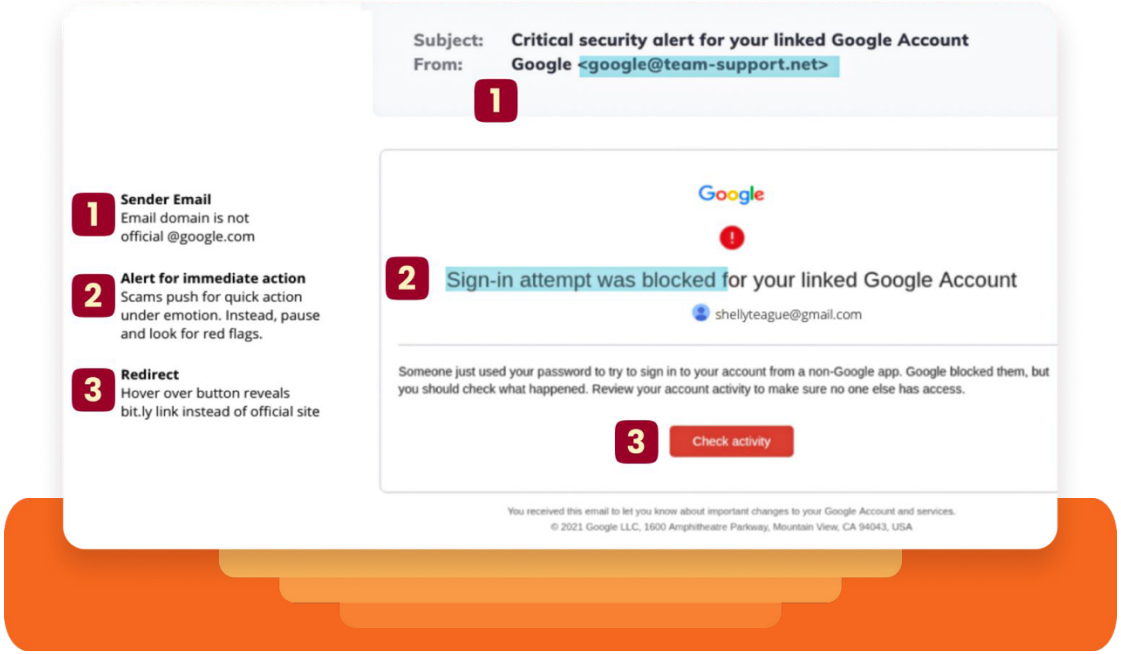


7 Types of Phishing Scams You Should Know About

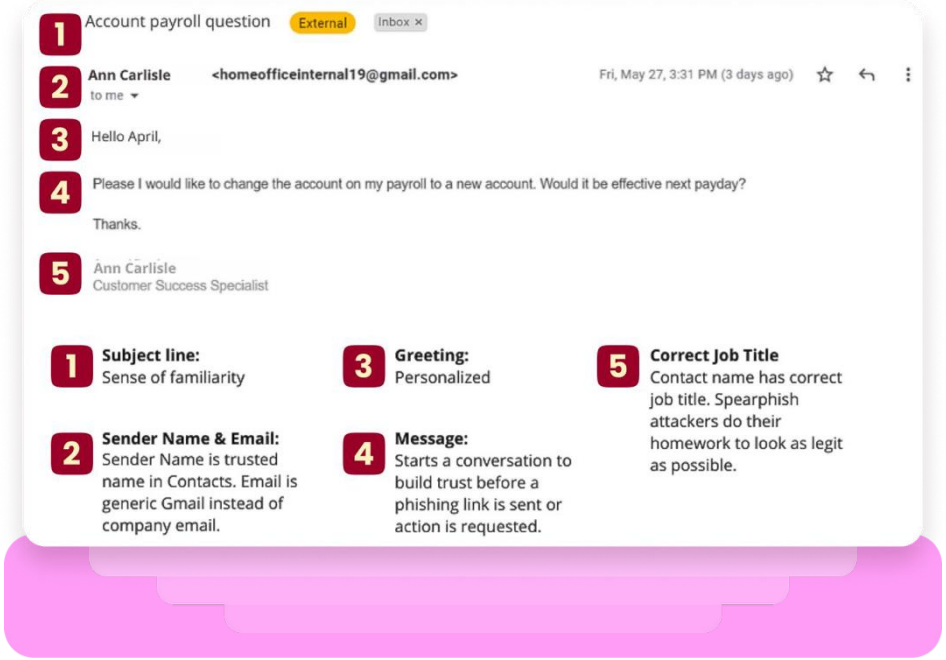


Email Phishing Scams

- It may look like an email from your bank, PayPal, Google, Amazon, or even your CEO



Spear Phishing Scams



- This is when they target you specifically. They have researched you, they know your family members, where you work, and who is your boss. The chances of fooling you are higher.

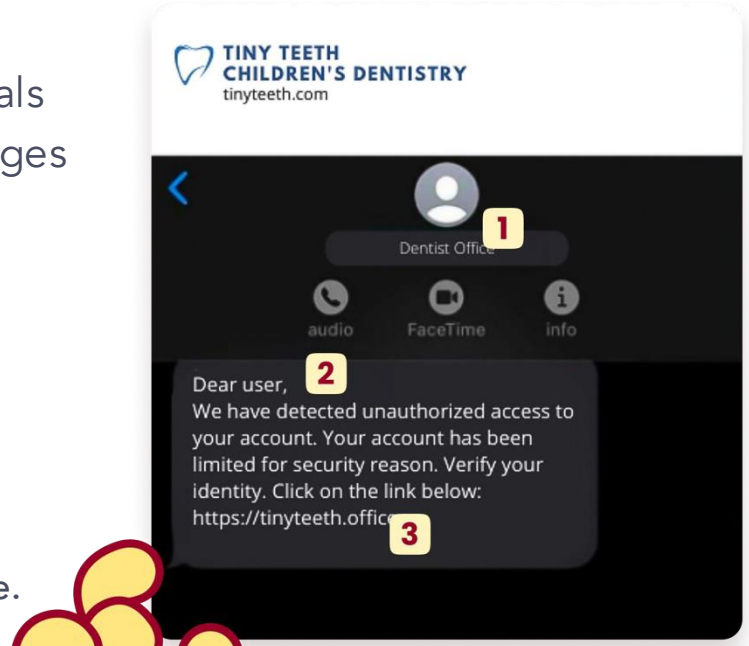
Smishing Scams

- These are text message phishing scams. Criminals know people respond to text and instant messages faster than email.

1 Look alike Contacts. Generic Contact Name is similar to Trusted Contact role.

2 Message conveys sense of urgency and fear.

3 Lookalike URL. Scammers buy lookalike domains similar to, but different from, the real company site.



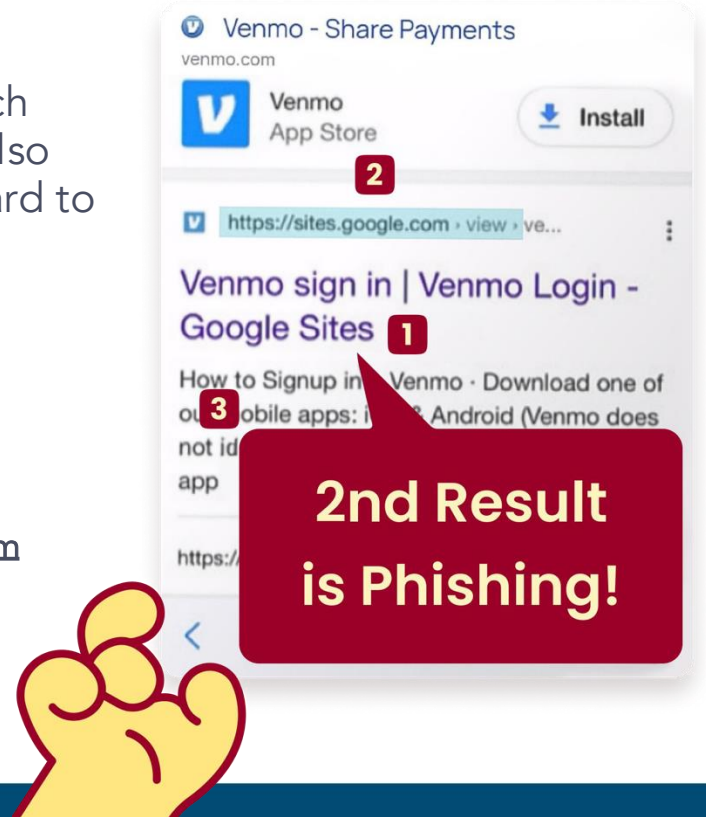
Google Search Scams

- You may be surprised, but some of the top search results in Google are phishing links. Scammers also invest in search engine optimization and work hard to rank their scam sites in the top search results.

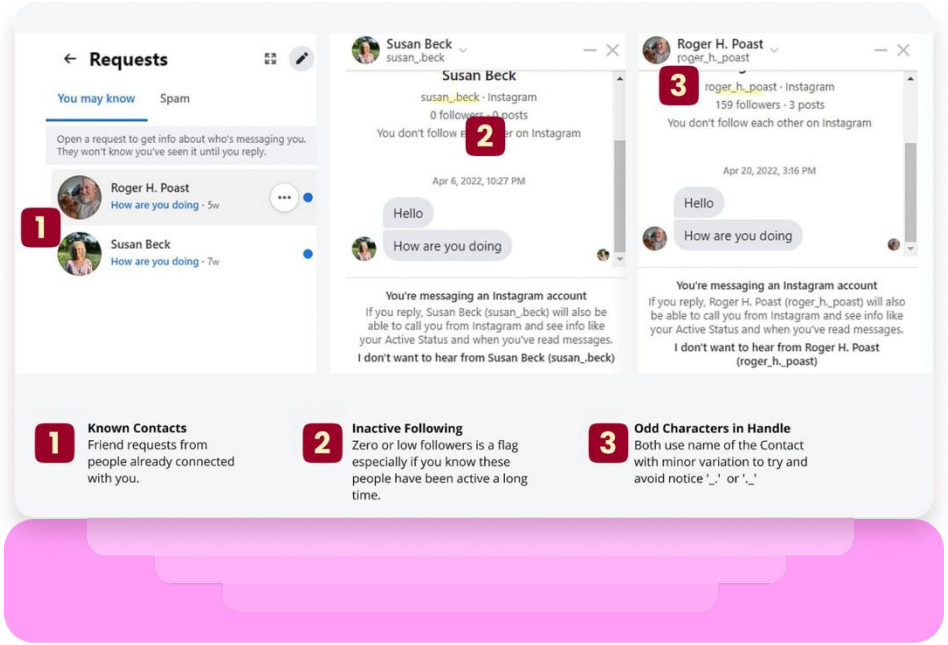
1 **Search Result Shows Brand**
Title displays correct brand name

2 **URL Mismatch**
Title says Venmo but URL is a generic sites.google.com

3 **2nd Result for Organic Search**
Even top search results can be manipulated for fake sites



Social Media Scams



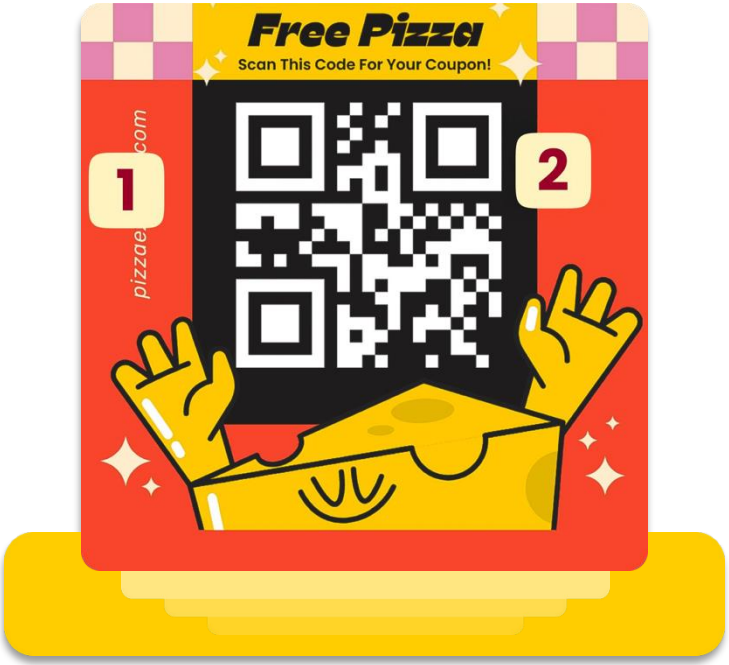
- Social media is full of fake accounts.
- It could also be a fake account with the same name and photo as one of your real friends that will later try to scam you.

QR Code Scams

- Who thought a QR code could be dangerous?
- They are everywhere, especially in restaurants. Criminals can place their own sticker over the legitimate one. So that when you scan it, you will be redirected to a fake site.

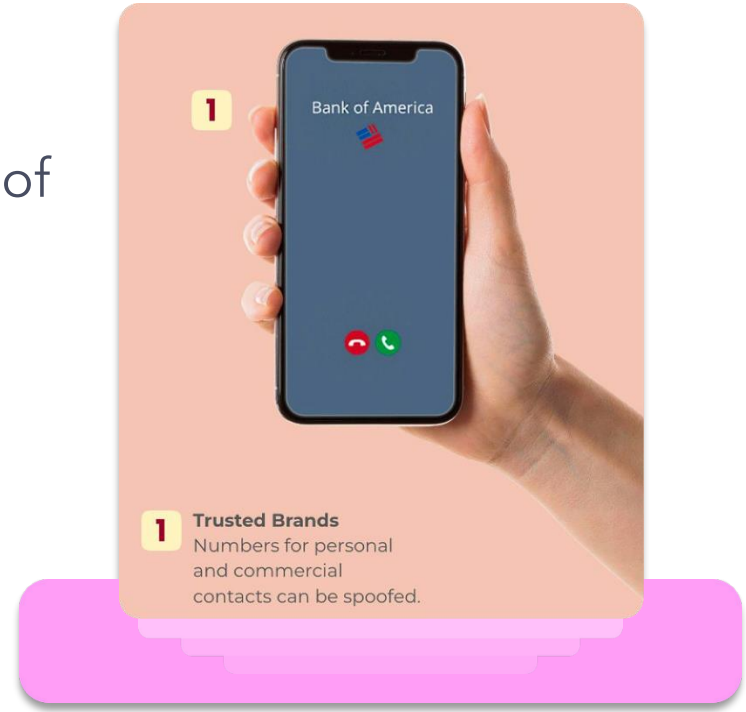
1 **Real URL**
Add legitimacy to ad

2 **QR Code**
Hides actual URL that directs to a fake site



Vishing Scams

- **Vishing** (voice phishing) is a type of phishing attack made over the telephone.
- **Scammers** can spoof a phone number that looks identical to a known number, like your bank.



What Helps Protect You From Phishing Attacks?

- If it's urgent, don't let the emotions cloud your judgment
- Call and verify! - Verify that you are talking to the correct person
- Check the address - Always check the email address and URL for spelling mistakes
- Policy Awareness Gap
- Look at the style of the message
- Ask Questions

How Long Will it Take to Crack Your Password?

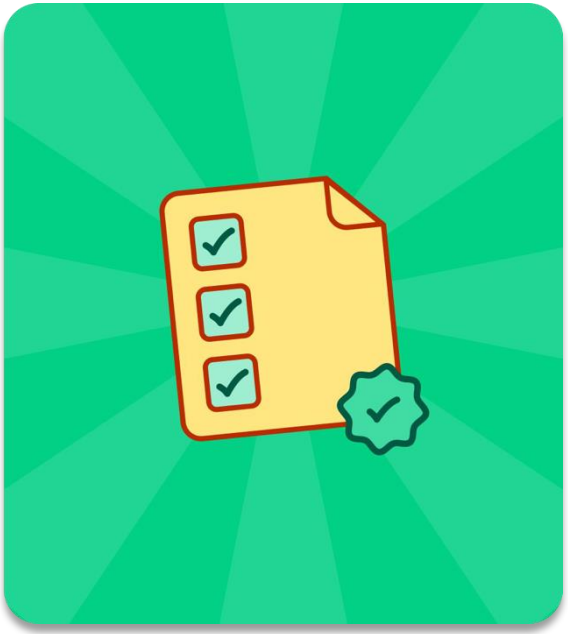
7 characters	**1 minute**
8 characters	**1 hour**
9 characters	**3-4 days**
10 characters	**7 months**
11 characters	**40 year**
12 characters	**2000 years**

Passwords include - Lowercase, Uppercase and Numbers

Passwords

How To Create a Strong Password:

- Passwords need to be **LONG!**
- **Use a phrase** (NO personal info like your name or B-Day)
- **DON'T** reuse passwords!



However…

- **11 BILLION** Accounts were stolen from hacked sites and apps.
- So even if you have a **STRONG PASSWORD**, it may still not be enough. You can check if yours was leaked at **haveibeenpwned.com**

And That is Why You Should Enable Multi-Factor Authentication

- This will help to protect your account if your password was stolen or leaked in a data breach.

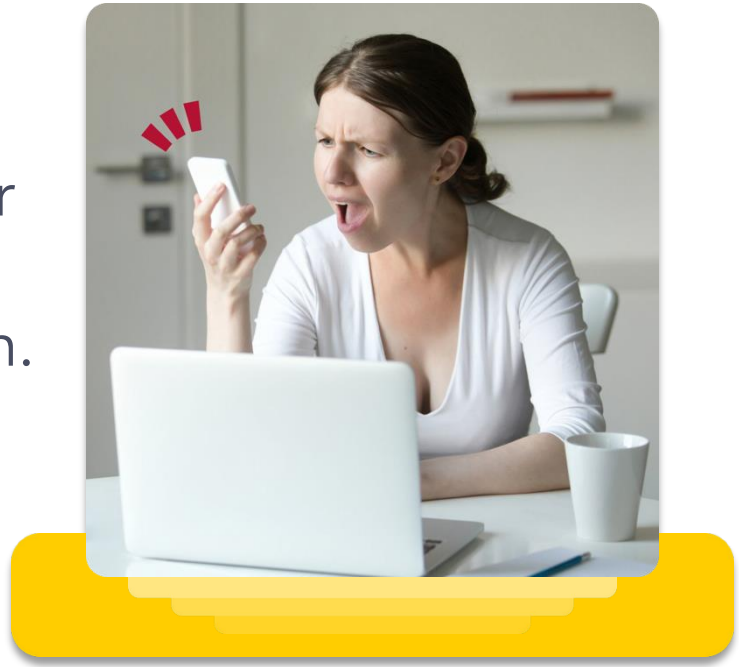
What Type of Multi-Factor Authentication to Use?

- Most common is text based (SMS), but it's the least secure
- It's better to use authenticator apps like Google or Microsoft Authenticator
- Or even better yet, a physical USB key

Malware

Ransomware

- When criminals hack your computer or network, lock you out, and demand a ransom to let you back in.



How to Avoid Ransomware

- **Don't download** files from random websites
- **Beware** of phishing emails with attachments (See phishing section)
- **Don't use** your company email or password for personal stuff
- **Don't store** password in text files or spreadsheets

Voice Cloning and Deep Fake

What is Voice Cloning?

- A mere **5-second** sample of your voice from social media is enough to clone your voice and impersonate you over the phone.
- **How do criminals use this?**
  - You receive a phone call from someone pretending to be your child, claiming they're in trouble and need money - but it's not really them.
  - You get a call from someone impersonating your boss, asking you to wire money - but it's not actually your boss.

How to Avoid Being Scammed By Voice Cloning

- **Establish a "Family Safety Word"** that only your family knows to confirm identity in case of emergencies.
- If you receive a suspicious call, hang up and **contact the person directly.**
- Use an alternative method, such as a text message or email, to **verify their identity. Don't trust a voice just because it sounds familiar.**

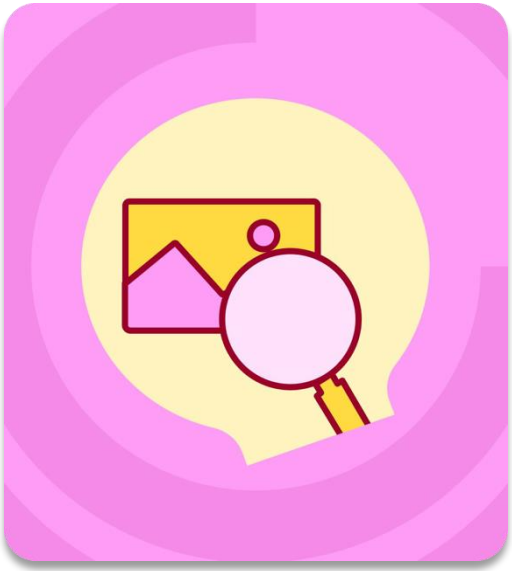
Let's Be Real – Deep Fakes Are Getting Scary Good!

- It's not about squinting at pixels or analyzing lighting. Forget trying to CSI every video frame.
- The Real Question:

👉 **Who's sharing this?**

The Playbook for Spotting Deep Fakes

- **Check the Source**
  Is this from the original creator, or just someone re-sharing it for clout?
- **Ask the Agenda Question**
  What's in it for them? Are they pushing a narrative, selling something, or stirring up drama?
- **Pro Tip:** Start treating "Agenda" and "Source" as the new metadata for everything you consume.



ChatGPT and Similar Apps

Tips For Using AI Tools Securely

- Be aware there are many fake AI apps and browser extensions out there that claim to be AI tools, but they are actually malware or phishing scams.
- Never enter any sensitive info or PII when using AI tools, it puts our data at risk.
- Remove any mentions of our organization, people or customers before using it.
- Always consult with the IT Team before using anything for work-related purposes.

REMEMBER: AI doesn't really understand the question!

Protect Your Mobile Device

- **Limit Apps** From Collecting Your Data
- **Disable Individual Apps** From Tracking You
- **Disable Apps** From Tracking You Even When You Are Not Using Them
- **Find Out** If You Are Sharing Your Location With Friends
- **Avoid Using a Simple PIN** to unlock your phone

Step by step guide on how to do this:
www.wizer-training.com/citizens/safeguard-your-privacy

Data Leaks

- **Share Google Docs carefully** — avoid giving "Editor" access to everyone and set expiration dates for external sharing.
- **Remove PII before using ChatGPT** or any external AI tool.
- **Avoid unauthorized plugins** — they can track your browser activity.

Wire Fraud

What is Wire Fraud?

It's when you're tricked into wiring money to a fraudulent bank account. For example:

- An urgent request to wire money from a criminal who impersonates your CEO through hacking your CEO's email account.
- They hacked one of your vendors and sent you an invoice with fake bank information.

If you're tricked into wiring money to a fraudulent bank account, the bank may not be there to help you. After all, it's you who transferred the money, not the criminal.

How to Avoid Wire Fraud

- **Call and verify** any money Request.
- **Call** a known number that you used before or from the vendor management system.
- **Verify** that the bank info match the one on file.
- **Call and verify** any request to change info on file, like phone number, address or bank info.

CYBER INCIDENTS – Who Should Know

- Notify Cyber Insurance
- Inform Local Police Department
- Report to Commonwealth Watch Center: 508-820-2233
- Email EOTSS SOC (eotss-soc@mass.gov)
- Strongly Encouraged under Executive Order 602/MA-CIRT
- FBI Internet Crime Complaint Center (IC3) https://complaint.ic3.gov/
- BEC with financial loss – file with www.IC3.gov report AND contact your financial institution immediately
- Others as outlined in your Cyber Incident Response Plan (CIRP or IRP)
- PERAC
- IT Provider
- Investment professionals
- Custodian
- Financial Institutions
- Board Counsel

STATE Resources

- **EOTSS Municipal Cybersecurity Awareness Grant Program (free):** Improve cybersecurity posture through end-user training, evaluation, and simulated phishing campaigns.
- **EOTSS Cybersecurity Health Check Program (free):** Cybersecurity Assessments to identify security gaps and an organization's ability to protect data and systems from cyber threats.
- **Community Compact Cabinet Grants Best Practices Program:** Opportunities to implement IT best practices related to planning and security.
- **IT Grant Program:** A competitive grant program focused on driving innovation and transformation at the local level via investments in technology using the transformative powers of IT
- **Municipal Fiber Grant:** The Municipal Fiber Grant program is a competitive grant program that will support the closing of critical gaps that exist in municipal networks.
- **State and Local Cybersecurity Grant Program** (SLCGP/MLCGP): Grants to assist municipal government in strengthening cybersecurity while reducing systemic cyber risk designated projects:
  - Multifactor Authentication (MFA) implementation, Cybersecurity Awareness Training, Migration to .gov domain
  - Tabletop Exercises (TTX), Cyber Incident Response Plan (CIRP)

Office of Municipal & School Technology (OMST)

Susan Noyes – Director Barnstable, Dukes, Essex, Nantucket Counties;
email: susan.noyes@mass.gov, phone: (617) 626-4403

- **Suzanne Zarges – MCAGP Program Coordinator, Worcester County;**
  email: cyberawarenessgrant@mass.gov
- **Stephanie Brown – Middlesex, Norfolk, Suffolk Counties, Cybersecurity Health Checks;**
  email: stephanie.brown5@mass.gov
- **Ralph DeLeo - Bristol & Plymouth Counties, Regional Planning Commissions;**
  email: ralph.deleo@mass.gov
- **Ken Wedge - Berkshire, Franklin, Hampshire, Hampden Counties, Cybersecurity Health Checks;**
  email: kenneth.wedge@mass.gov
- **Hannah Peterson, Municipal & School IT Analyst, Muni-IT-Dir SharePoint, Communications;**
  email: hannah.peterson@mass.gov

What To Do If You Suspect Your SSN Has Been Stolen (ssa.gov) – 1

- Identity thieves can use your SSN and other personal information to apply for loans and credit cards and open cellphone and utility accounts in your name. If you believe your information has been stolen and you may be a victim of identity theft, you can:
- Visit IdentityTheft.gov to make a report and get a recovery plan. IdentityTheft.gov is a one-stop resource managed by the Federal Trade Commission, the nation's consumer protection agency. Or you can call 1-877-IDTHEFT (1-877-438-4338).
- File a police report and keep a copy for your records in case problems arise in the future.
- File an online report with the Internet Crime Complaint Center (IC3) at ic3.gov. Its mission is to receive, develop, and refer cybercrime complaints to law enforcement and regulatory agencies.

What To Do If You Suspect Your SSN Has Been Stolen (ssa.gov) – 2

- Notify 1 of the 3 major credit bureaus and consider adding a credit freeze, fraud alert, or both to your credit report. The company you call is required to contact the others.
  - Equifax at 1-800-525-6285.
  - Experian at 1-888-397-3742.
  - TransUnion at 1-800-680-7289

What To Do If You Suspect Your SSN Has Been Stolen (ssa.gov) – 3

- Regularly check your credit report for anything unusual. Free credit reports are available online at AnnualCreditReport.com.
- Contact the IRS to prevent someone else from using your Social Security number to file a tax return to receive your refund. Visit Identity Theft Central or call 1-800-908-4490.
- To learn more, read our blog, Protect Yourself from Identity Thieves, and our Identity Theft and Your Social Security Number publication.

What else can you do to protect yourself:

- Create or sign in to your personal my Social Security account to check for any suspicious activity. If you have not yet applied for benefits:
- You should not find any benefit payment amounts, and you should be able to access your Social Security Statement and view future benefit estimates.

What To Do If You Suspect Your SSN Has Been Stolen (ssa.gov) – 4

- Review your Statement to verify the accuracy of the earnings posted to your record to make sure no one else is using your Social Security number to work.
- If you receive benefits, you can add blocks to your personal my Social Security account:
- The eServices block prevents anyone, including you, from viewing or changing your personal information online.
- The Direct Deposit Fraud Prevention block prevents anyone, including you, from enrolling in direct deposit or changing your address or direct deposit information through my Social Security or a financial institution (via auto-enrollment).
- You'll need to contact us to make changes or remove the blocks.

Contact Information

- Please send any questions to: Daniel.m.boyle2@mass.gov
- Thank you!


QUESTIONS?