Understand and Protect Against Modern Cyber Threats – For Anyone!

Cobb County Cyber Day 2025

Bill Martin
Cybersecurity Specialist

October 2025

Agenda

1 What Keeps You Up At Night?

2 How to Protect Yourself Online

3 How to Protect Your Devices

What Keeps You Up At Night?

Danger Danger - Alive and Well in 2025

Deepfake Incidents

Phishing Attacks

Supply Chain Attacks

IoT Vulnerabilities

Ransomware

Attacks on AI Systems

0-Day Exploits

Quantum Computing Attacks

State-Sponsored Attacks

The Cost

- Americans lost over $108M to AI scams in past year

- Avg loss $14,600 per incident, investment scams avg $55,00

- Deepfake fraud surge:
- 3,000% increase in 2023, now 6.5% of all fraud attacks
- 2024 – 4X increase in number of deepfakes world wide

- Deepfake losses in Q1 2025
- $200M+, avg $500K per business

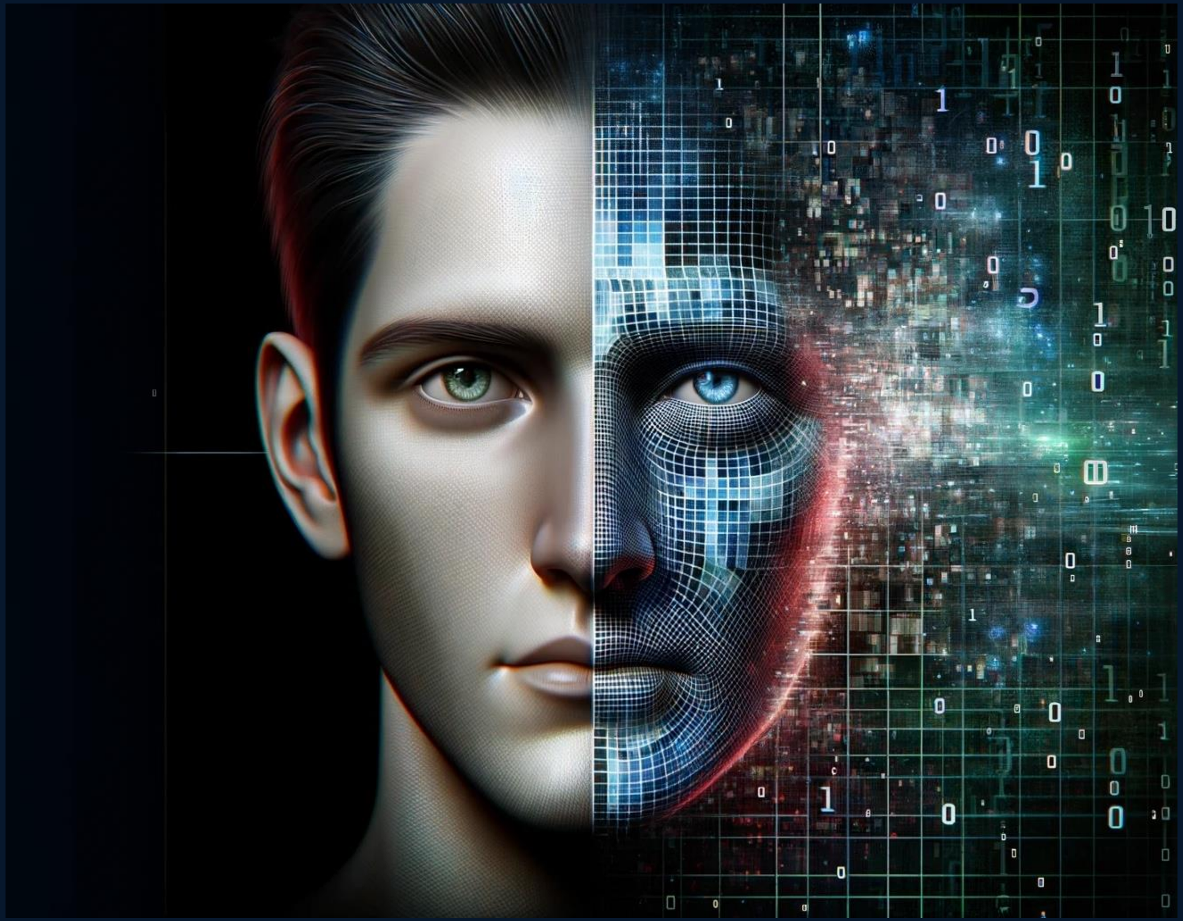
Deepfake Incidents

- What are Deepfakes?
  - Deepfakes are synthetic media where artificial intelligence manipulates or generates video, audio, or images to convincingly imitate real people
  - While sometimes used for entertainment, they are increasingly exploited for fraud, misinformation, and harassment

- Why Deepfakes are Dangerous?
  - Erode trust in real evidence (video/audio authenticity)
  - Enable fraud and financial scams
  - Cause reputational and emotional harm
  - Spread political misinformation at scale

Deepfake Examples

- https://www.youtube.com/watch?v=uqnljfe1Ems



Deepfake Incidents

- How to Spot a Deepfake
  - Look for unnatural blinking, lighting, or lip sync
  - Compare against trusted sources or official outlets
  - Use reverse image/video search to verify origins
  - Be cautious of urgent financial requests made via audio/video

- Protect Yourself and Your Organization
  - Verify requests through secondary channels before acting
  - Educate staff about AI-driven impersonation risks
  - Promote a culture of skepticism and fact-checking
  - Use AI detection tools when available

Phishing Attacks

- Generic email phishing (credential-stealing link)
  - Scenario: You get an email “From: IT Support” asking you to “verify your account” with a link to a login page that looks like your cloud provider
  - Red flags: generic greeting, mismatched sender domain vs display name, URL that doesn’t match the real site (hover to check), urgent language
  - Defense: Don’t click links – go to the service directly or use a bookmarked URL; enable MFA
- Spear phishing (targeted)
  - Scenario: An attacker researches you on LinkedIn, then emails you with personal details and a malicious invoice attachment
  - Red flags: personal details used to lower suspicion, unexpected attachments, request that bypasses normal processes
  - Defense: Verify sender by separate channel (phone), scan attachments in sandbox, enforce payee-change controls

Phishing Attacks

- Smishing (SMS phishing)
  - Scenario: A text claims there’s a problem with your bank account and includes a link to “fix it now”
  - Red flags: unsolicited SMS from unknown numbers, shortened links, requests for credentials
  - Defense: Don’t click – call the bank using the number on your card/statement
- Vishing (phone / voice phishing)
  - Scenario: A caller posing as tech support asks you to provide a one-time code or to install remote-access software
  - Red flags: caller pressure, requests for codes/MFA tokens, asking to install remote access
  - Defense: Refuse remote access unless pre-authorized; hang up and call the official support number
- Quishing (QR code phishing)
  - Scenario: A flyer hanging in a public place directing you to scan a QR code to learn more about an exciting upcoming event.
  - Red flags: requesting sensitive information or links with shortened URLs.
  - Defense: After scanning, carefully check the URL before clicking any links or entering credentials.

Don't Get Hooked by a Voice! Understanding Vishing Attacks

- Ever heard of "phishing" emails trying to trick you? Well, imagine that, but with a phone call!

- Vishing attackers are master manipulators, using social engineering to play on your trust, fear, or even excitement. They'll call you, often pretending to be someone important or trustworthy

- They might even "spoof" their caller ID, Their goal is to make you panic or feel pressured so you'll give up sensitive details like passwords, credit card numbers, or even transfer money.

Targeted Vishing Continued

- Examples:
- Your Bank: "Urgent security alert! Your account has been compromised, and we need your PIN to fix it!"
- The Government (IRS, Social Security): "You owe back taxes, and if you don't pay now, you'll be arrested!"
- Tech Support: "We've detected a virus on your computer; please give us remote access to fix it!"
- Even Your Boss or a Colleague: Using AI to mimic voices to get you to transfer funds or share sensitive company data.
- Family Member – claiming to have a family member hostage, or in jail, or something worse

AI Vishing Examples

- https://www.youtube.com/watch?v=z9zaMw6VLJg
- (play clip from 8:05 – 11:15)
- https://www.youtube.com/watch?v=pJZYd_65xs4
-

- Social Engineering Examples:
- https://www.youtube.com/watch?v=PWVN3Rq4gzw
- https://www.youtube.com/watch?v=Ic7scxvKQOo

Spotting the Red Flags

These sneaky calls often have tell-tale signs:

- Urgency & Threats: They demand immediate action, threatening dire consequences if you don't comply.
- Sensitive Info Requests: They ask for passwords, PINs, or full credit card numbers over the phone. Remember, legitimate organizations rarely ask for this!
- Unusual Language or Poor Quality: Robotic voices, strange background noise, or overly persuasive language can be a giveaway.
- Offers Too Good to Be True: "You've won a prize, just pay a small fee!"

How to Fight Back against Vishing

- **Hang Up!** If a call feels suspicious, just hang up. You don't owe them politeness.
- **Verify, Don't Trust:** If they claim to be from your bank or a company, *independently* call them back using the official number from their website or a trusted statement, not a number the caller gives you.
- **Never Give Out Sensitive Info:** No legitimate entity will ask for your full password, PIN, or multi-factor authentication codes over the phone.
- **Let Unknown Calls Go to Voicemail:** If you don't recognize the number, let it ring.
- Establish a “safeword” for family members, to confirm legitimacy
- Stay vigilant, trust your gut, and don't let a convincing voice trick you!

Give Feedback now to be entered in a Drawing

What is Quishing?

- **Definition:** Quishing is a type of phishing attack that uses QR codes to trick victims into scanning malicious codes that lead to fraudulent websites or trigger harmful actions.
- **How it works:** Attackers embed malicious QR codes in emails, posters, or websites, which when scanned, can steal credentials, install malware, or redirect to fake login pages.
- **Why it's dangerous:** Users often trust QR codes without verifying the destination, making quishing an effective social engineering tactic.

Quishing Examples

- https://www.youtube.com/shorts/08TCgEmuiAA

How to Spot a Quishing Scam

- **Check the source:** Only scan QR codes from trusted and verified sources.
- **Look for suspicious context:** Unexpected QR codes in unsolicited emails, messages, or public places can be a red flag.
- **Verify the URL:** After scanning, carefully check the URL before clicking any links or entering credentials. Look for misspellings or unusual domain names.

- **Avoid scanning QR codes that:**
  - Appear in unexpected places or unsolicited communications
  - Request sensitive information immediately
  - Lead to shortened or obfuscated URLs

- **Use security tools:** Employ QR code scanners that preview URLs and warn about malicious sites.
- **Educate users:** Awareness training on quishing risks and safe QR code practices.

How to Protect Yourself Online

Stay Safe Online: Password Management

12345678
PxH1#n!8

- Use Strong Passwords
  - Do not re-use passwords!
  - Use STRONG passwords – longer is better
  - Use a Password Manager
  - DO NOT save passwords in browsers
  - NEVER use default passwords

- Enable Multi-Factor Authentication (MFA) or 2FA
  - MFA is an extra verification/validation step
  - Ensure that only YOU have access to YOUR stuff
  - Protects you even if your password/account is compromised

👉 Think Before You Click. Cybersecurity is for Everyone.

Stay Safe Online

- Keep Devices Updated
  - If there is an update available, UPDATE
  - Enable auto-updates
  - Backup your data

- Beware of Scams
  - This is probably easier said than done
  - DO NOT click on links in strange emails or texts
  - Banks and governments NEVER ask for information via email or text
  - No emergency/critical decisions on an initial call – call back

👉 Think Before You Click. Cybersecurity is for Everyone.

Stay Safe Online: Family Protections and Controls

- Protect Yourself, Protect Your Family
  - Teach your kids about online safety – Use Apple Family, Google Family and other similar features to lock down websites and email and other communications
  - Teach your Family, especially our seniors – Facetime with screenshare is a handy tool
    - There are dangers online – talk about them
  - Keep your pin secret from your kids!

Staying Safe on Social Media

This Photo by Unknown Author is licensed under CC BY

- Review and tighten privacy settings to control who sees your info and posts
- Strong Authentication
- Use unique passwords and enable Two-Factor Authentication (2FA)
- Limit Personal Sharing
- Avoid posting birthdate, address, phone number
- Think Before You Click/Share
- Avoid suspicious links, unknown friend requests, risky quizzes
- Verify Friend Requests
- Confirm unusual money or urgent asks via separate trusted channel
- Report & Block

- Report suspicious profiles or content and block the user

Staying Safe on AI

- Stick with the major Gen AI LLM’s : ChatGPT, Copilot, Google Gemini
- Don’t train their models with your confidential financial or sensitive data
- AI can hallucinate
- AI can be biased, verify information

Protecting your Devices

How to Manage Your Home Smart Devices

Common Smart Home Devices

- Video Doorbells
- Smart outlets
- Smart Lights
- Security Cameras
- Streaming Devices
- Old Tablets
- Gaming Devices
- Smart TV’s
- Don’t leave settings on default, use a strong password
- If its too old, recycle it as E-waste, better to get rid of it and get something new than get compromised through an old device

How to Manage Your Old PC’s and Laptops

- **Back Up Your Data:**
- **Save Everything Important:** Transfer all essential documents, photos, and files to an external hard drive, cloud storage, or a new computer.
- **Wipe the Drive (Crucial!):**
- **Simple Deletion Isn't Enough:** Just deleting files or reformatting the drive doesn't truly erase data.
- **Consider Repurposing:**
- **Install a Secure OS:** If keeping it, install a modern, supported operating system like Linux Mint (as discussed) or a current version of Windows (if hardware allows).
- **Limited Use:** Dedicate it to less sensitive tasks, like a media server or a simple web browser.
- **Physical Disposal**

This Photo by Unknown Author is licensed under CC BY

Mobile Phone Best Practices

- Keep it Updated: Install OS and app updates immediately
- Smart App Use: Download only from official stores
- Strong Authentication: Use PINs/biometrics and enable 2FA
- Network Awareness: Avoid sensitive tasks on public Wi-Fi; turn off Wi-Fi/Bluetooth when idle
- Scam Vigilance: Don't click suspicious links or share passwords
- Prepare for Loss: Enable 'Find My Device' and back up data regularly

Thank you!