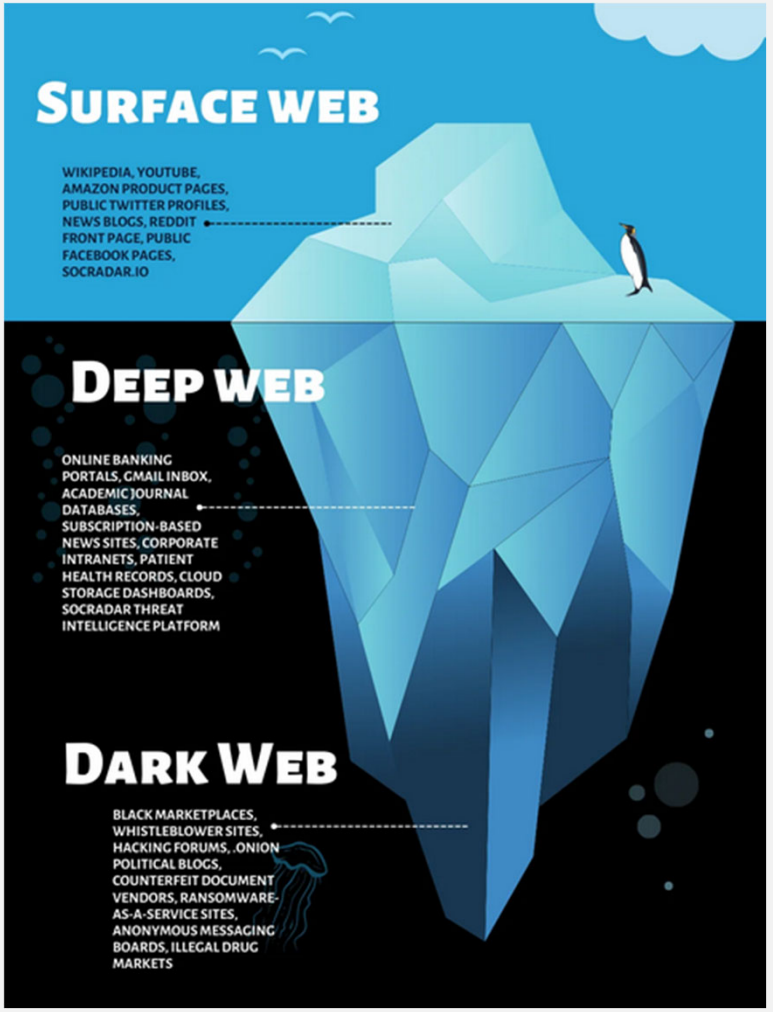
POJ SECURITY AWARENESS

March 2026

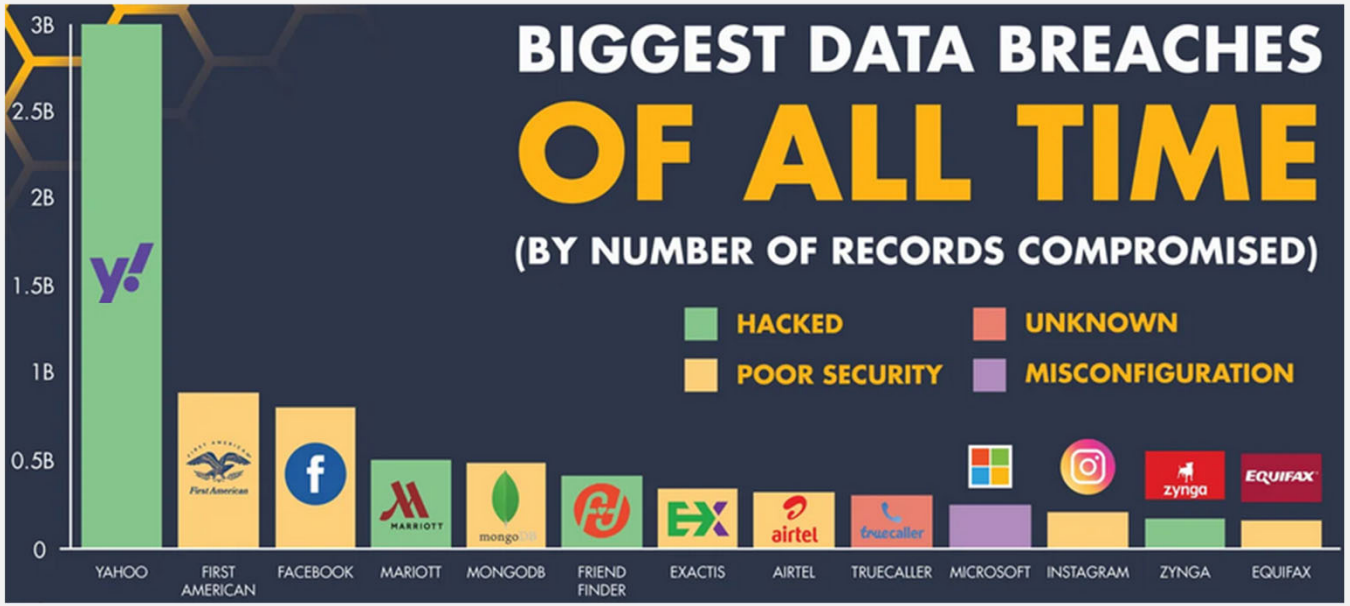
YOUR DATA IS FOR SALE ON THE DARK WEB (LIKELY FOR PENNIES)

- Some of the data comes from social media (often posted by you and me)
- Some of the data comes from public company compromises



CONSIDER EVERYTHING YOU POST ON THE INTERNET…

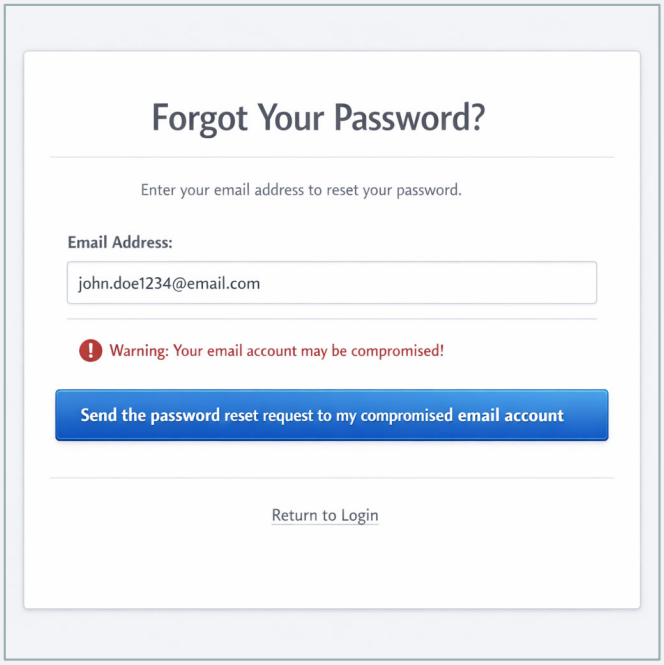
- As if you posted it on a bulletin board for the world to see



YOUR PERSONAL EMAIL ACCOUNT IS PROBABLY YOUR MOST IMPORTANT ACCOUNT

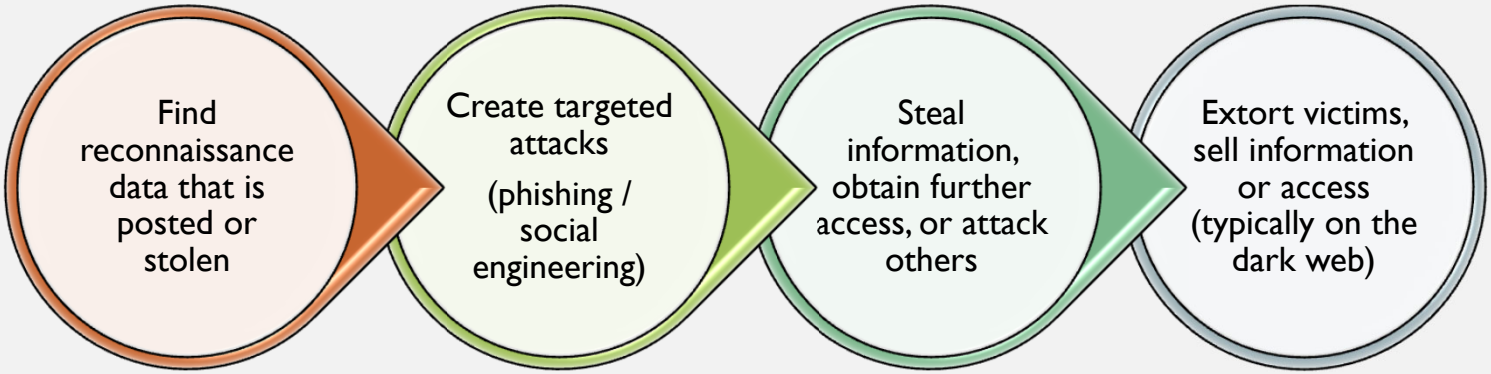
- Attackers don't need to steal your login information for your bank, investment, or any other important account – they just need access to your personal email

- Make sure you:
  - Enable MFA* on the accounts you care about
  - Use passphrases (>=18 characters)
  - Never use the same passphrase anywhere else



* Multi-factor authentication, also known as 2FA or two-factor authentication
Something you know (ex. Password) + something you have (ex. Access code)

TYPICAL CYBER ATTACK METHOD



AI VS. GEN AI

ARTIFICIAL INTELLIGENCE

- Analyzes existing data
- Finds patterns and anomalies
- Makes predictions or decisions
- Follows predefined rules and models
- Does not create new content

GENERATIVE ARTIFICIAL INTELLIGENCE

- Creates new, human-like content
- Generates text, images, audio, and video
- Mimics writing styles and voices
- Works at massive speed and scale
- Highly convincing and personalized

GEN AI AND SOCIAL ENGINEERING

- Generative AI (GenAI) amplifies the volume and sophistication of attacks
- Technology continues to make this easier (think Amazon but for nefarious purposes)
- Capabilities exist to automate attacks
  - Ex. Agents / chat bots on the dark web
    - Create phishing email using…
    - Obtain victim list from…
    - Create malicious software that...

WHAT IS PHISHING?

- Phishing is a social engineering attack where someone pretends to be a trusted source to trick you into acting
- Most phishing attacks start with or involve email because email messages:
  - Are easy to send (by the millions)
  - Are cheap
  - Only require one person to click or act
- Phishing attacks also include:
  - Voice calls
  - Text messages
  - QR codes
  - Social media messages…

According to Microsoft, ~3 seconds of your voice is enough to clone it

COMMON PHISHING OBJECTIVES

- Passwords (often to get to other services)
- Identities
- Money (direct theft or extortion)
- Sensitive / proprietary information
- Additional access (digital or physical)

Never use the same password anywhere else.

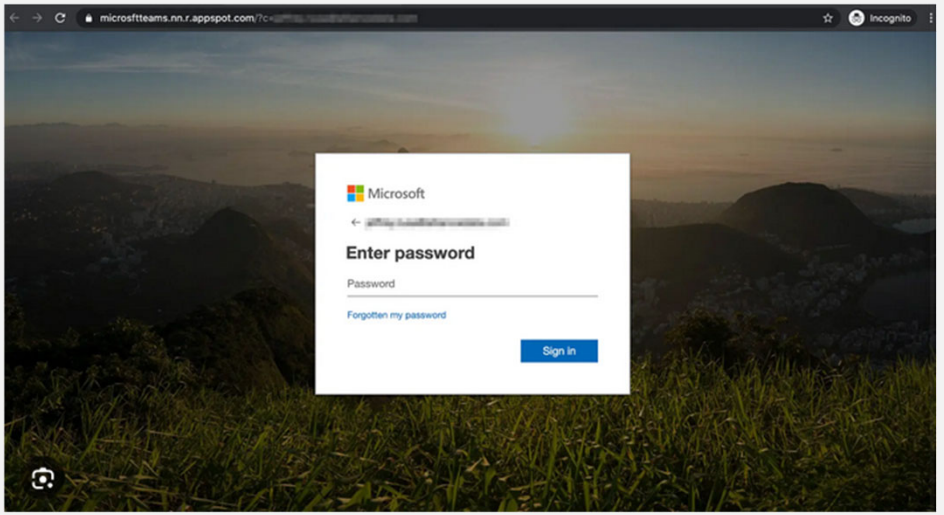
Ever.

WHY NON-PROFITS ARE TARGETED

- Non-profits often handle donor data, financial info, and personal information
- Smaller organizations typically lack:
  - Full-time IT and Cyber staff
  - Advanced security controls
  - Security awareness programs
- And…attackers are opportunistic

COMMON TYPES OF PHISHING MESSAGES

- Account issues / verification
- Loss of access
- Fake invoices
- Donation requests
- Leadership impersonation
- Package delivery notifications
- Discount offers
- Subscription notifications
- Fraudulent security alerts
- Parking
- Tolls (E-Zpass)
- Tax notifications



WHICH QR CODES ARE PHISHING?

PHISHING RED FLAGS

- Suspicious or unusual requests
  - This includes messages from someone you "know" and routinely communicate with
- Urgent or time-boxed communications
- Unexpected links or attachments
- Unusual message formatting
- ~~Poor grammar~~ Not written by a human
- QR codes in public locations
  - Good news: Credit card charges can be reversed
  - Bad news: Your phone number is "published"

POJ SECURITY CONTROLS

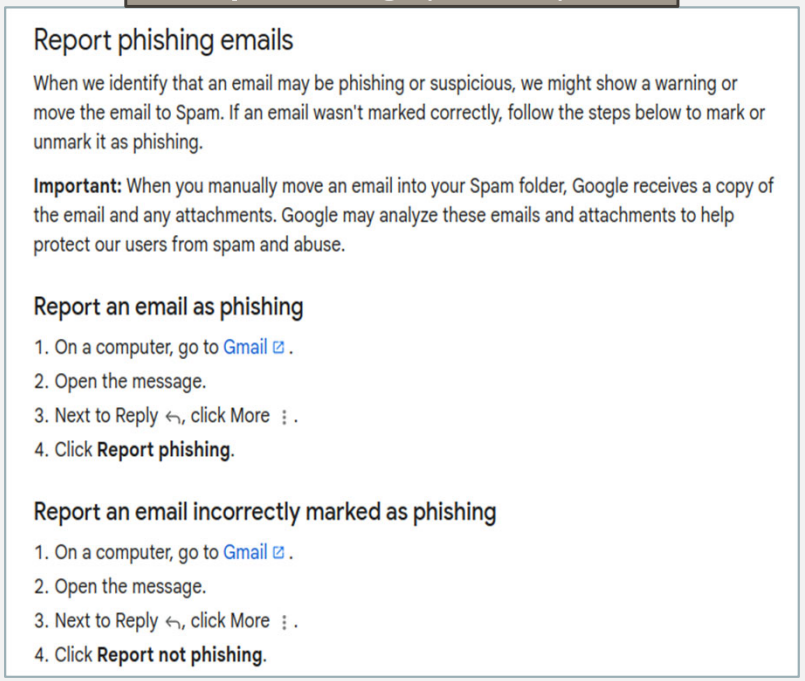
- Supported and hardened operating systems
- Workstation security policies
- Least privilege model
- Supported software / applications
- Monthly security patching
- Malware protection

- Drive encryption
- Multi-factor authentication
- Next-generation firewall
- Centralized logging
- Multiple data backups
- Network segmentation (separate networks for staff, guests, printers, etc.)

HOW TO SAFELY CHECK A LINK OR ATTACHMENT

- ~~- Hover over the link~~
- ~~- Look for misspellings or strange domains~~
- Never click on unexpected links or open unexpected attachments
- Contact the sender using a known good phone number from:
  - Your address book
  - A previously confirmed invoice
  - A trusted company website*

How to report email phishing (Gmail)



Report phishing emails

When we identify that an email may be phishing or suspicious, we might show a warning or move the email to Spam. If an email wasn't marked correctly, follow the steps below to mark or unmark it as phishing.

Important: When you manually move an email into your Spam folder, Google receives a copy of the email and any attachments. Google may analyze these emails and attachments to help protect our users from spam and abuse.

Report an email as phishing

1. On a computer, go to Gmail.
2. Open the message.
3. Next to Reply, click More.
4. Click **Report phishing**.

Report an email incorrectly marked as phishing

1. On a computer, go to Gmail.
2. Open the message.
3. Next to Reply, click More.
4. Click **Report not phishing**.

* Note: Beware Google search results and "Sponsored" links

YOU PROBABLY GET PHISHED EVERY DAY

1. Don't respond to or act on unsolicited messages
2. Use separate email addresses for sites you really care about

   (and use MFA, preferably with an authenticator app)
3. Open a web browser and type in the name of trusted websites instead of clicking on links, opening attachments, or scanning QR codes
4. Verify links and attachments are legitimate by calling the sender using a trusted phone number
5. Limit what you post on the Internet

   (it will be used to target you with attacks)

FINAL QUESTIONS

Are you keeping your personal devices updated with the latest software?

Are you avoiding the installation of apps based upon popularity? (TikTok is bad)

Do you have a backup copy of your most important data saved in a secure (alternate) location?

Are you downloading files only from trusted & verified websites?

Are you avoiding links, attachments, and QR codes in unexpected messages?

Are you locking your device when you walk away? And properly securing them in your car, office, etc.?

If you answer "no" to any, you are going to be hacked
(or you will have a hard time recovering from a cyber attack)

GOOGLE SEARCH

Be aware of the information on you and your church that can be easily found online.