THREAT LANDSCAPE

- Cybercrime: Use of the internet to commit a crime, either directly (drain your bank account) or indirectly (selling personal information).

- Spear phishing: integrating recipient-specific personal information into an email with the intent of tricking the recipient into taking an action.

- Doxxing: online searching and publishing a target’s private information for a malicious purpose.

- Child Identity theft: Using a child’s SSN and other identifying information to open lines of credit for cash or products. May go undetected for years.

- Swatting: reporting a fraudulent hostage situation to law enforcement, sending armed swat teams to the victim’s home or business.

Keep Learning

Center for Internet Security
[https://www.cisecurity.org](https://www.cisecurity.org)

SANS Institute OUCH!
[http://www.securingthehuman.org](http://www.securingthehuman.org)

STOP. THINK. CONNECT.
[https://www.stopthinkconnect.org](https://www.stopthinkconnect.org)

FTC Phishing

FTC Computer Security
[http://www.consumer.ftc.gov/topics/computer-security](http://www.consumer.ftc.gov/topics/computer-security)

FTC Identity theft:
[https://identitytheft.gov/](https://identitytheft.gov/)

AARP Fraud Watch Network
Helpline: 1-877-908-3360

Krebs on Security
[https://krebsonsecurity.com](https://krebsonsecurity.com)
**TECHNOLOGY BEST PRACTICES**

- Use reputable anti-virus, and set to auto update
- Keep your tablet and cell phone apps and OS up to date
- Encrypt mobile devices with a password (iPhone) or settings (Android or Samsung)
- Use complex, 9+ character passwords
- Don’t log into a secure site while on a public network
- Respond immediately if notified that your account information has been changed

**SHOPPING BEST PRACTICES**

- Don’t shop with a debit card
- Don’t shop (or bank!) from an email link. Use your bookmark or type in the URL
- Don’t use non-bank ATMs
- Use the chip card where it is accepted. Complain to the merchant when it is not

---

**Empower Your Password Portfolio to Evade Password Attacks**

- Follow the best practices listed in this brochure!
- Change your passwords regularly
- Use diverse characters - upper and lowercase letters, numbers, special characters (# ^ & !)
- The longer your password, the stronger the protection
- Don’t use public information such as your name, address, birthday
- Use a phrase, not a word
- Pick a unique password for each site that stores account info, credit card or SSN (Amazon, Sunpass, bank)
- Pick a single password for those will little to protect (i.e. Publix)
- If you keep a password log, use clues, not the password itself
- Use text-messaged one-time PINs if your vendor offers it

---

**THE EMAIL CONNECTION**

- 66% of cybercrime incidents used phishing as part of the attack plan.
- 23% of recipients open phishing messages. 11% click on attachments.
- A phishing campaign of 10 emails will have a >90% chance of at least one person clicking a link.

---

**WHY EMAIL?**

- Designed to work the same way on every computer, tablet and phone, simplifying the technical challenge for malware delivery
- Source of valid addresses
- Rich data set for social engineering
- Used to create zombies, plant key loggers that captures your key strokes

---