Security Awareness
A Non-Technical Presentation

NOACSC

Ray Burden, Executive Director

ray@noacsc.org

We all are Responsible

- Everyone has a role in maintaining security for your district
- Access to sensitive data
  - Student and Staff
- Access to the Internet
- The “bad actors” have evolved
  - Viruses are still out there but..
  - It’s about your data
  - It’s about your Userids

- Trick Bots
- Malware
  - Malicious Software
- Find a place to hide and capture data traffic
- District Examples
  - $12 million
  - Amazon Purchases

What you can do – my top 2

- **Logins**
  - Protect them like they are your children
  - Multiple logins are a way of life today
    - Work, Banking, Netflix, Amazon, USPS, etc.
  - Keep your passwords secure
  - Do not use a shared login
    - Taking a personal and professional risk

- **Email**
  - Beware of scammers
  - Don’t open email from a sender you do not know
  - Delete, delete, delete
  - Refrain from checking personal email at work on district owned devices

What you can do – continued

- Clean Desk Policy
- BYOD – Personal Devices
  - Should be on Guest Network
  - Unlimited Data Plans
- Removable Media
  - Random thumb drive
  - External Hard Drive

- Safe Internet Habits
  - Strong passwords
  - Keep personal info sharing limited

Some other items

- Don’t use email to transfer student and/or staff data
- Use secure file-sharing
- NOACSC offers a secure file-sharing service at no charge
- For Administrators:
  - Cyber-Liability Insurance

- Keep your district’s name out of the news
- 80%+ data breaches are caused by human error

Thank you

- Resources:

- https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

- https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/