Navigating the Internet in a Crazy Digital World

(Or Scary Stats and Simple Things You Can Do to Stay Safe to Avoid jerks, Bigots, and Manipulative Conspiracies)

Discussion Points

1. Who Am I and What Am I Talking About?
2. Risks and Statistics
3. Bullies, Trolls, Traps, and Techniques
4. Protecting Your Organization
5. Protecting Yourself
6. Learning Opportunities & Resources

Risks and Statistics

(Or There are Some Really Scary Stats, Dorothy!)

Stats...

1. In the US, around **7.5 million people** experience cyberstalking each year. [Link]
2. **61% of cyberstalkers use everyday tools** like smartphones, text messaging, and email, and around 10% use malware or phishing to hack into their victims' accounts. [Link]
3. 16% of cyberstalking victims 18 to 24 years old **said perpetrators shared sexually explicit photos** or videos of them without their consent. [Link]
4. **Only 29% of stalking victims** report the crimes to police. ***Say what?!?*** [Link]
5. According to an FBI agent, when a young person visits an online forum for a popular teen singer or actor… parents can be reasonably certain that **online predators** will be there. It is believed that more than 500,000 pedophiles are online every day. [Link]

And More Stats!

6. According to a study in the journal JAMA Psychiatry, Black children and teens who experience racial discrimination online **may develop symptoms related to PTSD**. [Link]
7. Traditional bullies are **2.5 times more likely to cyberbully** than someone who has never been bullied. [Link]
8. According to the Cyberbullying Research Center, **only 40% of cyberbullying victims report** it to their parents, and only 30% report it to a teacher. [Link]
9. **Roughly 70% of LGBTQ+ adults encountered harassment online** and fully 51% have been targeted for more severe forms of online abuse. [Link]
10. Study shows that **60% of teens between ages 13-17 agreed with 4 or more conspiracy** statements compared with 49% of adults. For teens who spend 4+ hours/day, the figure reaches **69%**. ***Yikes!*** [Link]

Bullies, Trolls, Traps, and Techniques

(Nasty People and Their Methods)

Bullies, Trolls and Traps

Bullies

1. Typically target via social media.
2. Often your children won't share their pain.

Trolls

1. Target to elicit a response. (Think "troll" as in fishing.)
2. Love social media. It's what made them!

Traps

1. Target children where they hang out and feel safe.
2. Build trust, create private talks, test boundaries, and then sexualize the relationship.

Methods and Techniques

- ✓ **Phishing** attacks to plant attack software on your computer.
- ✓ **Malicious websites** to drop dangerous payloads.
- ✓ **SMishing** - SMS messages to build trust or destroy one's self confidence.
- ✓ **Imposter scams** to trick you for whatever the nasty persons plans might be.
- ✓ **Social media stalking or trolling** to create an emotional response such as fear and uncertainty.
- ✓ **Hate mongering** - You can figure this one out...
- ✓ **Watering hole phishing** to catch children and people where they hang out.
- ✓ **Personal Attacks** to cause pain.

Protecting Your Organization

(It All Starts with Good Policies, Training and Testing)

Good Policies, Training and Testing

Policies

1. Establish email use policies which include no mixing of personal and professional accounts.
2. Require various tools to protect your staff and network (see Slide 14 below).

Data Privacy Policies

1. Never, never, NEVER send protected info via email.
2. Require protected information to be stored in a secure cloud environment.

Training and Testing

1. Arrange cyber-awareness training sessions to build knowledge.
2. Get an assessment of your DP risks and test your IT infrastructure.

A Little Extra: Email Phishing

How to Spot an Attack AND Avoid Being Tricked

1. **Check the email address** and look for **sloppy layout** and/or **spelling and grammatical errors.**
2. **Check the greeting.** “Dear customer” or a generic greetings can be a give away.
3. **Look for spoofed hyperlinks** by hovering your mouse over the link to see if it is different from the destination displayed in the message.
4. **Treat all attachments and links with caution**!!!
5. **Be suspicious of any message** that requests you to click a link or open an attachment!!!
6. **Beware messages promoting a sense of urgency** or dire consequences if you don’t act immediately.
7. **Contact the person or the organization** using a different, validated method like a phone number you already know OR look up the organization’s website ‘Contact Us’ information. Never use the message’s links or contact information!!!
8. **Do not provide personal or sensitive information** in response to a message.

Protecting Yourself

(A Few Simple Tech Skills Can Serve You Well)

Good Planning and Zero Trust

Secure Your Devices and Browser

1. **Automatically update your OS** and other critical software.
2. Use **antivirus software** such as Windows Security.
3. **Use a VPN** such as NordVPN or ProtonVPN. Avoid FREE VPNs!
4. Use a **password manager/vault** such as LastPass or BitWarden.
5. **Use the Firefox browser** and add extensions such as HTTPS Everywhere, NoScript, SquareX, and UBlock.
6. Also **configure your browser** for heightened security.
7. Use a **data breach scanner** such as HaveIBeenPwned.com.

Practice Zero Trust

1. Don’t trust anything that is sent to you. Always verify and test.

Password Guidelines...

Prudent Password Guidelines

The key to creating and storing strong passwords...

1. **Length:** Minimum of 15-64 characters. Use a password generator (and vault), if possible. This is the single most important factor.
2. **Complexity:** Mix it up with upper case/lower case, spaces, characters and numbers!
3. **Unique:** DO NOT REUSE PASSWORDS. Need I say more? For “fun”, check “**Have I Been Pwned?**” for your email and password.
4. **Uncommon:** Don’t include well known phrases, quotes, or lyrics.
5. **Don’t Share:** Yes, I need to say this: Don’t share your passwords.
6. **Use a Password Manager/Vault:** But make sure that your passphrase is very long to protect the master login. Do the same for your email account since that is usually the achilles heel for most secure systems. **Recycle every 30 day**s.

Learning Opportunities and Various Resources

Learning Opportunities

Locally

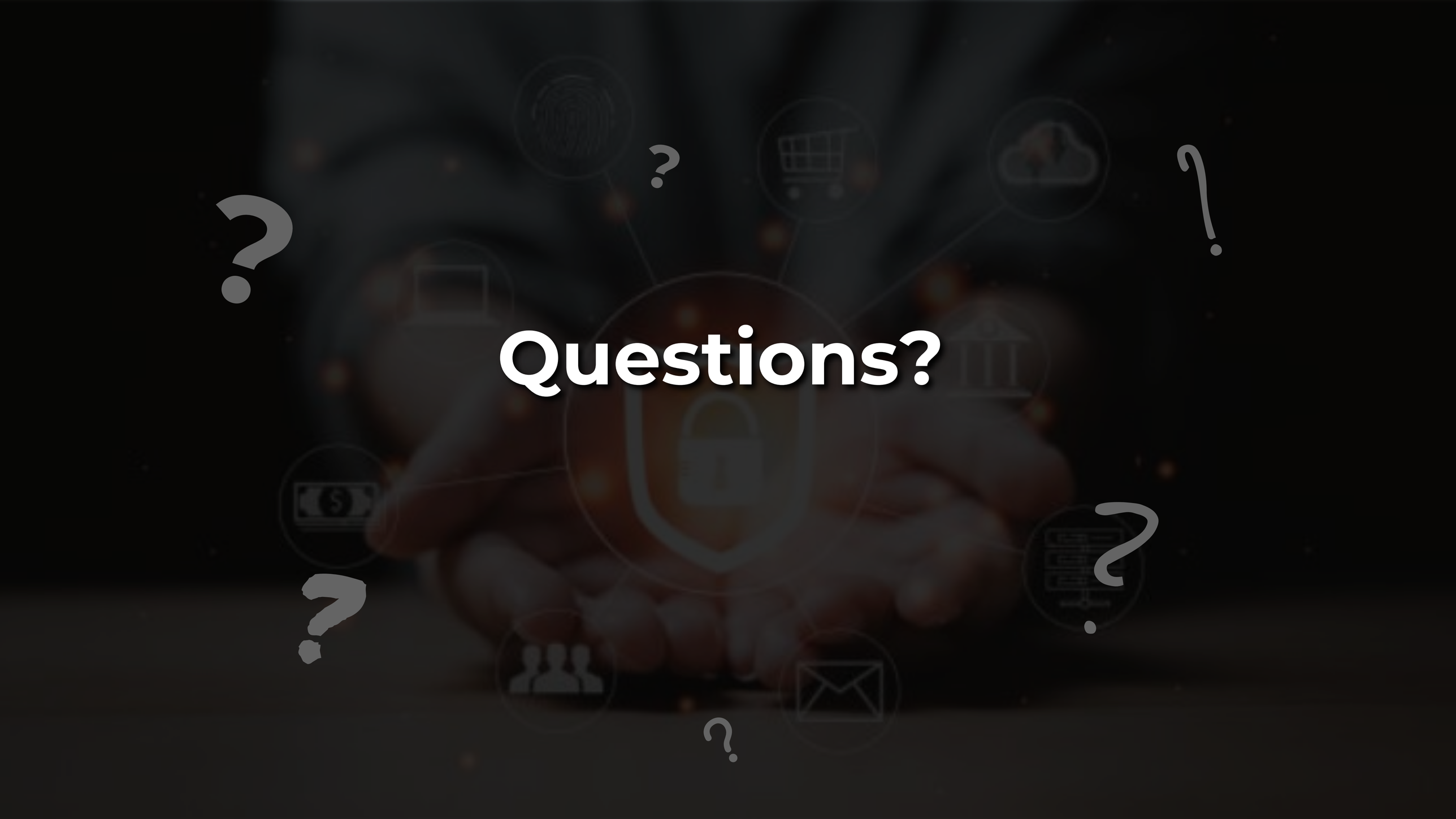
1. **AntiguaRecon** - Teaches ethical hacking skills such as pentesting, vulnerability assessments, open source intelligence (OSINT), and simulated phishing.

The World

1. **TryHackMe.com** - Online cybersecurity training both free and paid.
2. **HackTheBox.com** - Same as above.
3. **PortSwigger.com** - Same as above.
4. **YouTube/Google** - Tons and tons of content.

Resources and Tools...

1. **Have I Been Pwned?:** Excellent tool that you can use to research if your phone or email has been included in a data breach.
2. **Password Manager Options:** The list provided here covers a range of options identified by PCMag. Each has its adherents and detractors. Your final decision should include feedback from your IT Department (which might require a specific option) and/or consideration of the security solution you are using on your computers since the solution might include its own password manager.
3. **Top 10 VPNS:** Again, the list is offered by PCMag and you should apply the same decision-making logic as recommended above for the password manager.
4. **Cybersecurity Awareness Quizzes:** Whether for your staff, or for self-training, these quizzes are good options for testing your knowledge, or that of your staff.
5. **CyberBullying Research Center:** - Resource for understanding the topic, getting information, and most importantly, getting help.
6. **Online Predator Ebook:** Ebook put out by the Beau Biden Foundation, an initiative to protect children from on and offline predators.


Questions?

More to Come!!

Don’t forget tomorrow’s *Cybersecurity Awareness Training*!

Where? Right here!

When? 1 PM - 3 PM

Who? Me.

HOW TO REACH US

+1 268.764.8362

antiguarecon.com

adam@antiguarecon.com