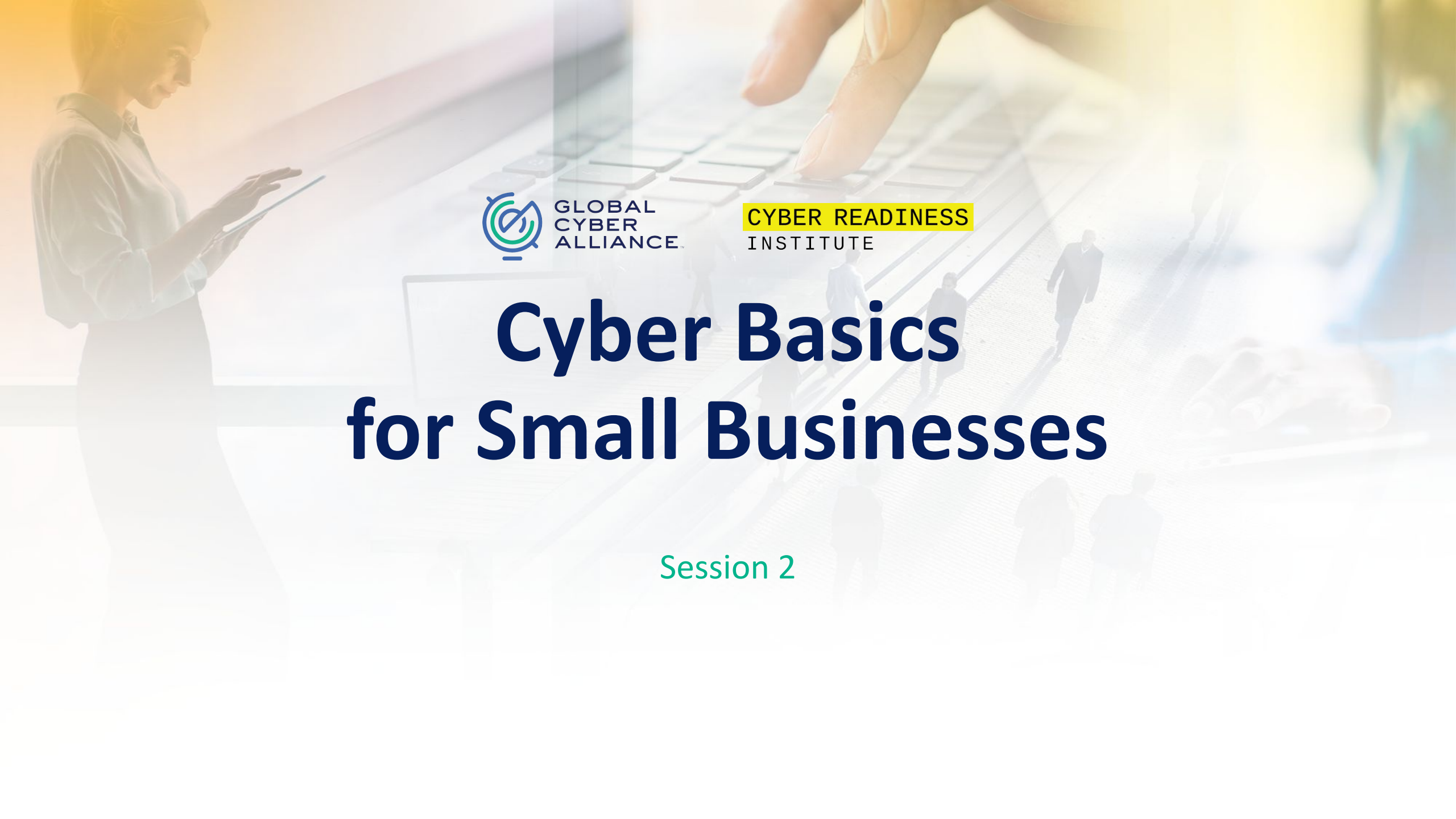


GLOBAL CYBER ALLIANCE

CYBER READINESS INSTITUTE

Cyber Basics for Small Businesses

Session 2

Today's Agenda

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Prevent Phishing and Malware

- Introduction
- Anti-virus
- Domain Name System (DNS) Filtering

Week 1 Refresher

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Know What You Have and Update Your Defenses

- Complete the inventory for all your devices, software, and accounts
- Ensure all your software is up to date – patched to the latest revision
    - Set to automatically update where possible
- Identify third parties who can remotely access devices within your environment

Beyond Simple Passwords

- Ensure all your accounts use strong and different (unique) passwords
- Enable 2FA for all your accounts (where 2FA is supported)
- Check your remotely accessible devices for admin/admin default settings.

Prevent Phishing and Malware

Prevent Phishing and Malware

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Over 90% of cyber-attacks start with a phishing email!

They are NOT easy to spot

- Is it really from someone you know? It may look genuine – same email address, logos and format

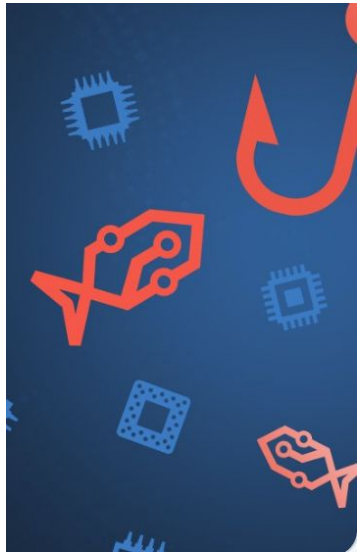
- Act Quick - ‘headline news’ or a job you’ve just done

- They may have called your company or checked online to personalize the email

The attacker will do whatever they can to make their email **appear genuine** and **enticing –** they are very good at it

Definitions

- **Phishing**: Untargeted. May relate to recent news stories, tax year, common organizations used by many – *'spread the net wide and catch as many as you can'*
- **Spear-Phishing**: Targeted. Designed to look like a person or organization you know, some research needed – *'fishing with a rod and line'*
- **Whaling**: Highly targeted. Reconnaissance required, may be tracking movements for months before making a move – *'high rewards - the big one'*



Phishing - via email

Smishing - via SMS

Vishing - via telephone

What Harm Could A Phishing Email Do?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Create a **backdoor** into your system

- **Email** your contacts

- Corrupt or hold data to **ransom**

- **Change** bank account details

- Install a **Keylogger** to listen in

- Change contact details

Do not interact with a suspicious email

Always double-check requests, using **KNOWN, GOOD** credentials

The Consequences are Severe:

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- 2/3 of SMBs have suffered a cyber-attack in the past 12 months (Ponemon Institute)
- Global cost of malware is $2 trillion USD (Forbes)

Do you have processes in place?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- **Mandate or Payment Diversion Fraud**:

  - An existing supplier changes their banking details
  - A new supplier provides banking details
    Use an alternate method to check - i.e., phone a known contact.

- **CEO Fraud**:

  - Email pretending to be the CEO/senior authorized person - payment to be made to…
    Instill a policy that it's good to double check - family businesses often operate on trust and few checks. Create an 'I will never….list'

- **Business Email Compromise (BEC)**:

  - From a compromised email account sending emails 'from inside their system'
    Use DMARC to help prevent the initial compromise. Check your email (forwarding) settings.

Prevent Phishing and Malware: Anti-Virus

Anti-Virus(AV): How does it work?

- Each virus has specific characteristics (a signature)

- AV checks for these and stops the virus infecting computer
- New viruses are created - a **'zero-day attack'** = no protection

- AV software updates (time lapse) = now protected

Some anti-virus software may look out for unusual behavior (heuristics)

It is important AV is **up to date**. New viruses are constantly being developed

Prevent Phishing and Malware

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Install AV for computers and mobile devices
- Ensure devices and accounts are updated
- Conduct on-going user awareness training

Prevent Phishing and Malware: DNS Filtering

What Is DNS?

- Domain Name System (DNS) = the internet's 'phone book'

- New domains are created and registered by Registrars (e.g., GoDaddy..)

- Unique Domain Name (globalcyberalliance.org) assigned a unique set of numbers (IP address 192.297.10.27)

❖ *It is estimated that of the 200,000+ new domains registered daily across the globe up to 70% may be intended for malicious activity. (Palo Alto Networks)*

Criminals often register **look-alike** website domain names (i.e. rn instead of m)

They may hide behind a 'Click Here' link in an email

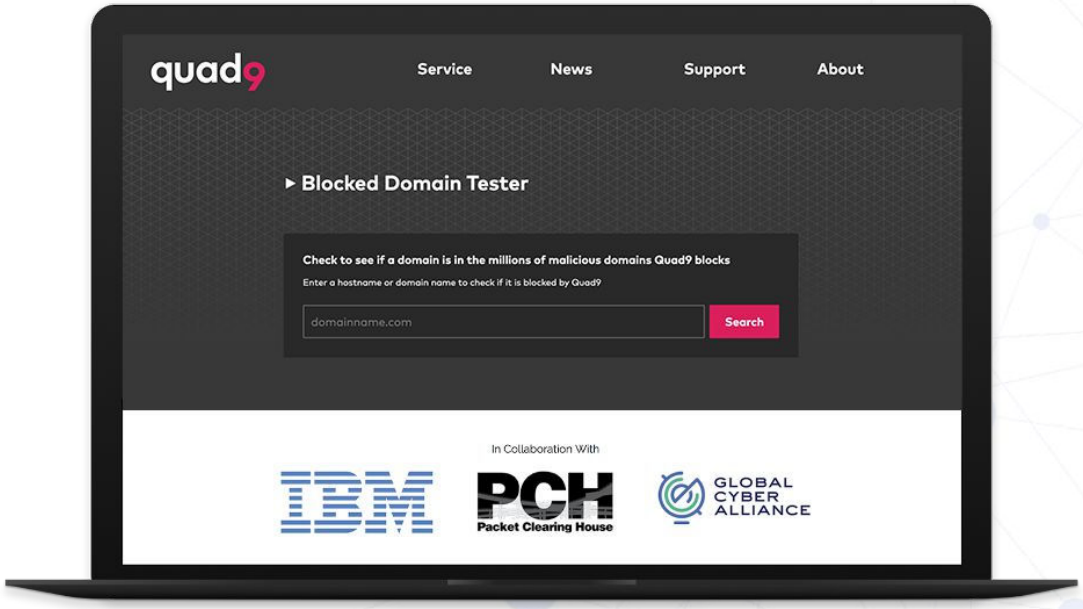
What is DNS Filtering?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

DNS filtering blocks access to known bad websites

Quad9: Checks IP address against threat intelligence feeds.

- Blocks if **known bad**
- Average **60+ million blocks** per day.
- **Easy** to set up



Anti-Virus and Quad9

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

+ quad9

Anti-virus and DNS filtering (Quad9) work together to provide layers of defense

Prevent Phishing and Malware:

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Be cautious of emails, clicking on links and downloading attachments

- Check (and install) anti-virus on devices and mobiles

- Regular Staff Awareness Training - *They are the network guardians*

- Configure Quad9
  - On your devices
  - Connect app on your Android device
  - Quad9 on your routers: https://www.lifewire.com/how-to-change-dns-servers-on-most-popular-routers-2617995

CRI Additional Resources

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Cyber Readiness Program

https://cyberreadinessinstitute.org/the-program/

- Covers four core focus areas: Authentication, Software Updates, Phishing, and USBs and Removeable Media
- Trains a cyber leader

CRI Resources

https://cyberreadinessinstitute.org/resources/

- Remote work guides, ransomware guide, and additional resources and information for SMEs

CRI Starter Kit

https://cyberreadinessinstitute.org/starter-kit/

- If you aren't ready to start the full program, there are some helpful tips and tricks in this kit.

GCA Additional Resources

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

GCA Cybersecurity Toolkit for Small Business

https://gcatoolkit.org/smallbusiness/

- Prevent Phishing and Malware

GCA Learning Portal

https://edu.globalcyberalliance.org/bundles/small-business

- Protect Against Phishing & Malware

GCA Community Forum

http://community.globalcyberalliance.org/

Cyber Basics Resources

https://gcatoolkit.org/cyber-basics-for-small-businesses-training/

Q & A

Join Us Next Week for Session 3

April 28

8am EDT - 1pm BST - 2pm CET

12pm EDT - 6pm BST - 7pm CET

Backup and Recover

Why backups for your data and systems are important for your business

Protect Your Email and Reputation

Know what DMARC stands for, why it's important, and what attacks it mitigates; be able to check your own email domain to see if DMARC is enabled