GLOBAL CYBER ALLIANCE

CYBER READINESS INSTITUTE

Cyber Basics for Small Businesses

Session 1

Trainers

- **Shehzad Mirza**, Director of Operations, GCA

- **Lessie Longstreet**, Global Director of Outreach and Partner Engagement, CRI

- **Gill Thomas**, Cybersecurity Toolkit for Small Business Lead, GCA

- **Rodney Lee**, Technical Project Manager, GCA

Opening Remarks by Mastercard

➢ **Sandy Condellire,** *Senior Vice President, Cyber & Intelligence Solutions*

Today's Agenda

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Overview of Cyber Risks

Learn what threats your business faces

Know What You Have

Why having an inventory of your assets is critical

Update Your Defenses

What is patching and why it is important

Beyond Simple Passwords

Understand why strong passwords are important and what additional steps you can take to secure accounts

Cyber Risk: What Is It?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Your ‘cyber risk’ indicates the risk of business loss due to a technology systems failure. This includes:
  - Financial loss
  - Disruption to business operations
  - Legal and liability issues or reputational damage

- Risk comes from many places:
  - Information on conducting online fraud is easily accessible
  - Attack vectors have increased due to connectivity of systems and volume of data available
  - Cybercriminals monetize attacks by:
    - Stealing and selling data
    - Holding the data hostage and demanding a ransom

Cyber Risk: Types of Attackers

Script Kiddies

- Bragging rights, not intending to cause harm – it's a game

Financially Motivated Attackers

- Make money, intentional – it's their 'job'

Hacktivists

- Publicity, to highlight a cause - it's their belief (it may be political)

Nation States

- Spy, finance activities, control infrastructure– it's 'cyber warfare'

Cyber Risk: How They Attack

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Loopholes, ‘open doors’, unguarded ways in

- A phishing email

- A flaw in a piece of software or operating system (vulnerability)

- Use of common malware

- User complacency … it will never happen to me/I’ll do that tomorrow...

‘No degree necessary’ for the attackers - anyone can have access to advanced tools which are available to buy or rent online (as are the services of more sophisticated ‘black hats’)

Cyber risk has reached epidemic proportions for small businesses:

- Almost **30% of data breaches** in 2020 involved small businesses (Verizon DBIR)
- **A single cyber incident can cost $200,000** (Hiscox's 2019 Cyber Readiness Report)

Know What You Have

Know What You Have

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

You cannot protect what you do not know you have:

- **What** is in your **IT** environment?
- **What** and **Who** is on your network?
- **Anything** that **connects** to the **internet**?

✓ Laptops
✓ Tablets
✓ Servers
✓ Accounts

✓ Smart Phones
✓ Printers
✓ Application
✓ Email…

? IoT Devices
? Old Accounts
? Old software

? CCTV
? Old equipment
? 3rd Party Access

CREATE YOUR INVENTORY

Who Needs Access for Business as Usual?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

1. Set **minimum** access levels for **effective** productivity
2. Restrict access (admin, user, none) to reduce potential damage from:
   - Insider threats - intentional and accidental
     - *Deliberate action*
     - *Employee blackmailed to extract information*
     - *Impact of opening a phishing email*
     - *Accidental deletion or corruption of data*
   - Network/physical segmentation
     - *Insecure devices on the network (i.e., IoT devices)*
   - Third-party access
     - *Attack delivered through a third-party action (deliberate or unintentional spread of a virus)*

Update Your Defenses

Update Your Defenses

- Cybercriminals look for weaknesses and flaws (known as vulnerabilities) that can be used to gain access to systems or spread malicious software. Malicious actors could gain access to your company's financial accounts, your customers' data, and much more.

- You can help protect against this by updating your defenses (i.e., keeping your systems, devices, and data updated).

- Manufacturers and software developers regularly release security updates for their operating systems and applications to address newly discovered weaknesses or vulnerabilities. These fixes are usually referred to as patches, and the process is known as patching.

Protect What You Have!

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- **Security Updates or ‘Patches’**
  - Issued by manufacturers and developers to fix coding loopholes/vulnerabilities

Set to Auto Update

+

Remove what you do not need
Replace end of life / unsupported
(Know what you have!)

Update Your Defenses

Encrypt your data. Encryption is the process whereby data is converted from a readable form to an encoded form. This encoding is designed to be unintelligible except by parties that possess the “key(s)” to reverse the encoding process.

Secure your website. If hackers gain access to the website they could intercept or steal data, change its contents, infect the website with malware, or take over operations. Any of these could have a devastating impact on your organization's ability to operate. You should run regular checks on your website (known as scans) to identify vulnerabilities and potential weaknesses.

Know What You Have and Update Your Defenses

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- 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

ENSURE YOUR INVENTORY IS KEPT UP TO DATE

Failure to update computer systems puts your business at risk

Beyond Simple Passwords

Beyond Simple Passwords

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

One of the common methods criminals will use to gain access to your accounts, network, and information is to log in as you.

Are you using the same password across multiple accounts?

Access to one account gives access to all

- A cheap, modern laptop and program can crack a password faster than ever.
- Long passwords/passphrases and additional protections are a must

How Can Passwords be Cracked?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Brute force attack: Using computing power to automatically enter all possible combinations - ***Use long passwords or passphrases and characters***

Dictionary attack: A form of brute force attack that uses known dictionary words/phrases or common passwords - ***Use memorable words/passwords but not common ones or ones that might be associated with you***

Credential stuffing: Once one account has been compromised they will try the same username/password elsewhere - ***Use a different password for each account***

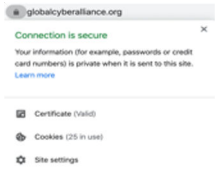
How Can Passwords be Cracked?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- **Social engineering**: Trick people into revealing passwords – i.e. phishing emails. ***Never give out your password, or parts of it, to anyone.***

- **Manual guessing**: Personal information, i.e., names and dates of birth are used - ***What does the web and SM say about you? Steer clear of 'PII' in passwords***

- **Shoulder surfing**: In a public place, or even at your desk - ***Who's behind you? Where's that CCTV camera?***



- **Interception**: Passwords can be intercepted as they are transmitted over a network - ***Check for https green padlock.***
  but note https DOES NOT infer a genuine website just an encrypted link

Creating a Strong Password

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

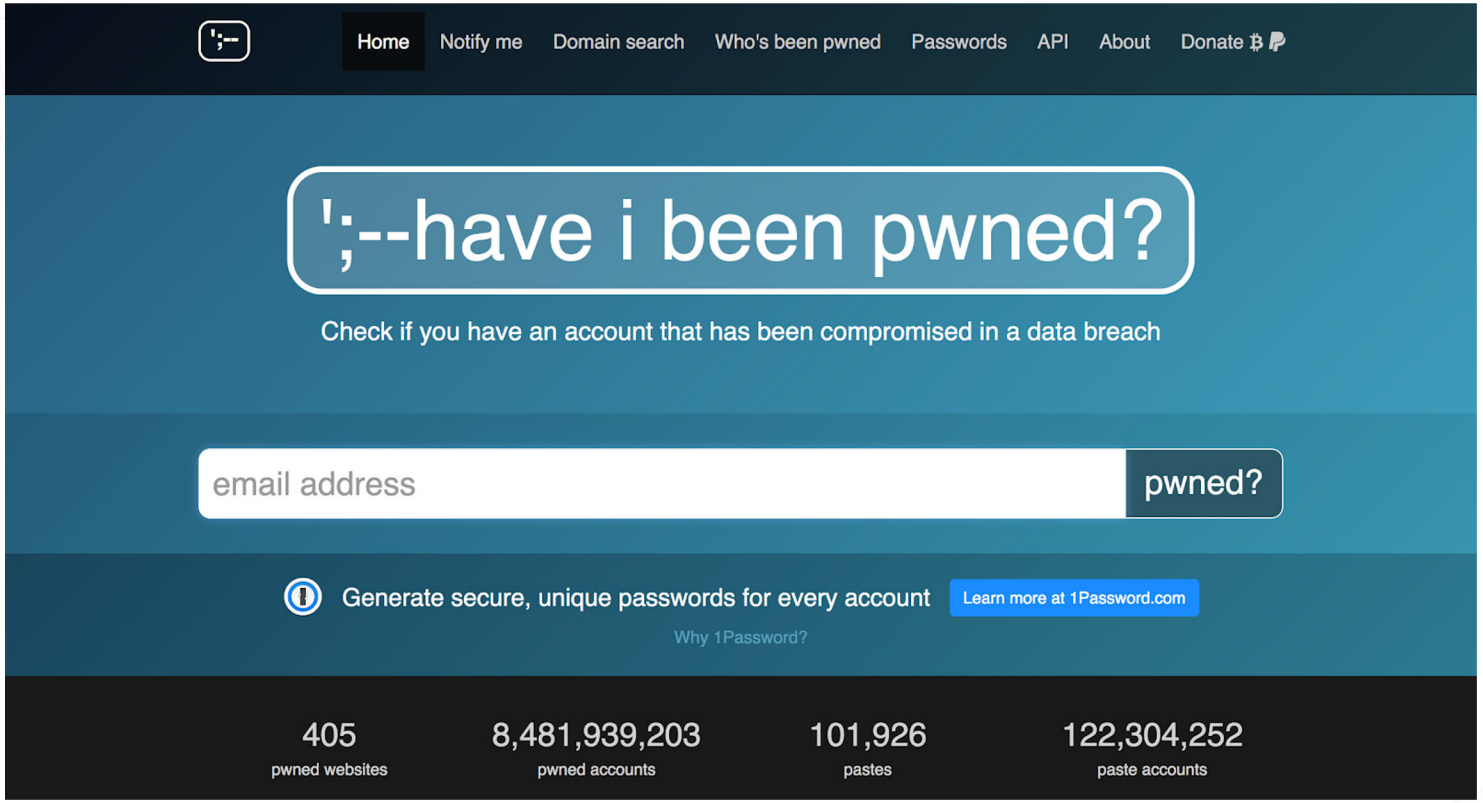
Passwords should be long, complex and memorable

- Ensure a company-wide policy
- No personally identifiable information
- **Do NOT use your birthday or anniversary date as PIN/password**
- Use a different password for every account
- Use a password manager if you prefer

Have You Been Breached?

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Have your accounts been breached already? Check at:
https://haveibeenpwned.com/



Change password immediately if so! *(On all accounts affected)*

Ensure all passwords are unique!

Multi-Factor/Two-Factor Authentication (MFA/2FA)

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Provides increased levels of protection against compromise

Something you know:

- A password

AND something you have:

- A token (Google Authenticator, Okta, RSA) ***Preferred method**

- A verification code sent to your phone (SMS)

- A fingerprint or face (biometrics)

Using MFA/2FA makes it **much harder** for an attacker to gain access to your accounts

Beyond Simple Passwords

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

- Install Authenticator App (examples: Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile)
- Ensure all your accounts use strong and different (unique) passwords
- Check if any have been compromised and change passwords if they have
- Enable 2FA for all your accounts (where 2FA is supported)
- Check your remotely accessible devices for admin/admin default settings. Always change guessable default passwords before first use.

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/

- Know What You Have, Update Your Defenses and Beyond Simple Passwords Toolboxes

GCA Learning Portal

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

- Understanding Cyber Risk for Small Business
- How To Inventory Your Devices, Apps and Accounts
- Software Updates and Business Security
- Creating Strong Passwords and Two Factor Authentication

GCA Community Forum

http://community.globalcyberalliance.org/

Q & A

Join Us Next Week for Session 2

April 21

8am EDT - 1pm BST - 2pm CET

12pm EDT - 6pm BST - 7pm CET

Prevent Phishing and Malware

Overview of viruses and other malware; how they can infect your systems; how to protect against attacks; understand Domain Name System (DNS) security; how it helps prevent users from going to infected websites; how to use Quad9 tool for DNS security