Cybersecurity, Charities, and Nonprofits

The GCA Cybersecurity Toolkit for Mission-Based Organisations

Gill Thomas Director of Engagement
Capacity & Resilience
1st October 2024

GLOBAL CYBER ALLIANCE

GCA Founders

CITY OF LONDON POLICE

DISTRICT ATTORNEY NEW YORK COUNTY

CIS Center for Internet Security®

GCA Cybersecurity Toolkit for Mission-Based Organizations

Free

Straight forward

Global

Private

Sponsored by Public Interest Registry

In partnership with Global Cyber Alliance

Essential cyber hygiene will significantly reduce your risk of attack

https://gcatoolkit.org/mission-based-orgs/

Nonprofit/Charity Cyber Risk: Why

- Have funds and data
  - Donor information
  - Vulnerable community data

- Donation appeals
  - ‘Predictable’ annual campaigns or disaster response

- Minimize ‘back office’ costs to maximize ‘frontline’/mission impact
  - Transparent reporting
  - Often lack IT specialist skills, resources

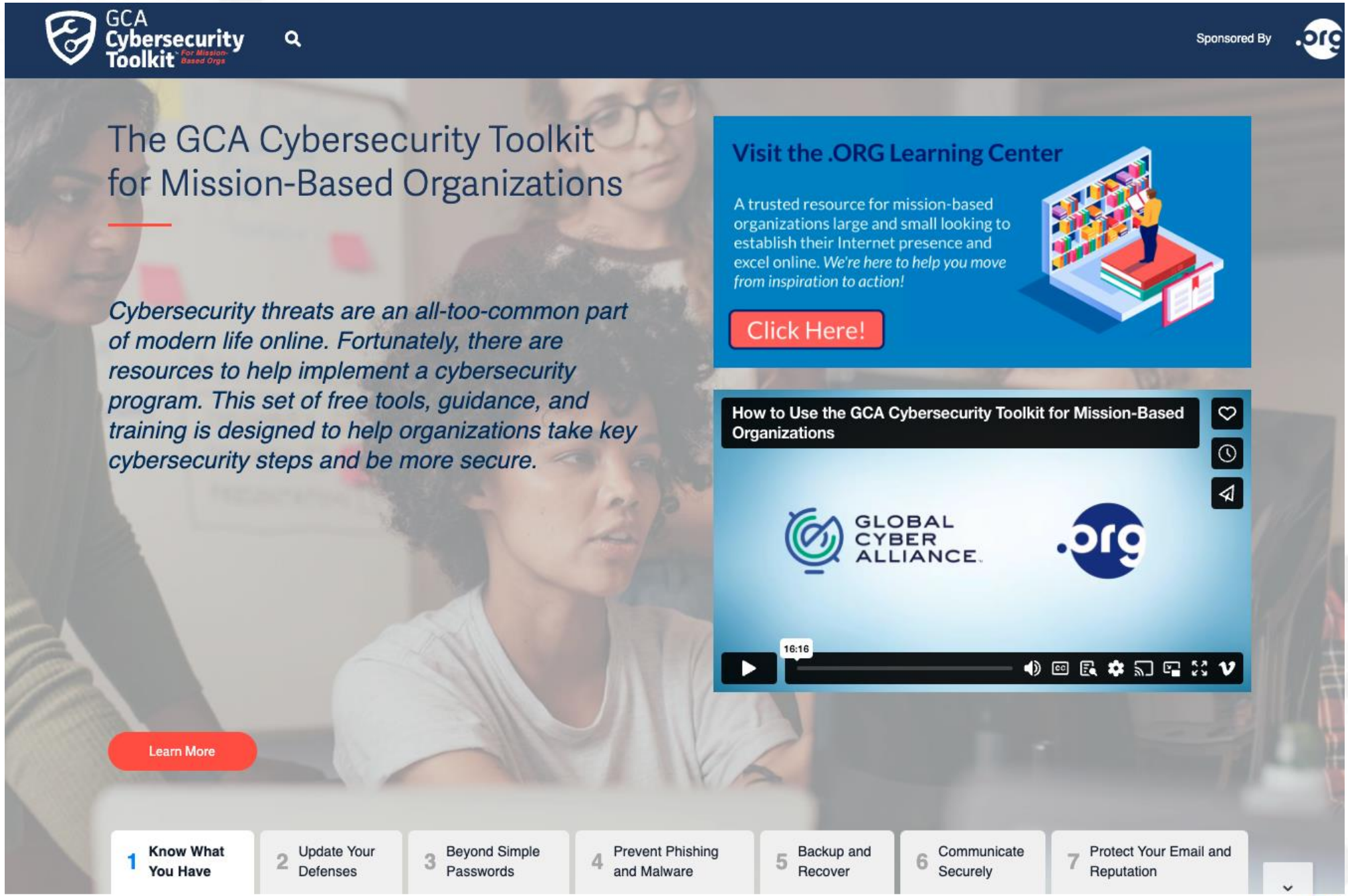
- Believe in the mission
  - Could be targeted because of the mission or just because of systems in use
  - But cyber criminals do not care

- A soft target verses ‘for profit’ counterparts

Nonprofit/Charity Cyber Risk: How?

- Loopholes, ‘open doors’, unguarded ways in
- A phishing email
- A flaw in a piece of software or operating system (vulnerability)
- Fake websites and 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’)



GLOBAL CYBER ALLIANCE

LINK

GCA Cybersecurity Toolkit - guided steps to better cybersecurity

1. Know What You Have
Inventory

2. Update Your Defenses
Software updates, encryption, website checks

3. Beyond Simple Passwords
Strong, unique and 2FA

4. Prevent Phishing & Malware
Anti-virus and DNS Security (Quad9)

5. Backup and Recover
Configure and schedule backups

6. Communicate Securely
Calls SM, IM, emails, browsing

7.Protect Your Email & Reputation
DMARC and website checks

Cyber Awareness and Education Courses

STEP 1

Know What You Have

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**?

Remove the not needed, unsupported and noncritical

- ✔ Laptops
- ✔ Printers
- ✔ Accounts
- ✔ Smart Phone
- ✔ Servers
- ✔ Email…
- ❓ IoT Devices
- ❓ Old Accounts
- ❓ Old software
- ❓ Old equipment
- ❓ CCTV*
- ❓ 3rd Party Access*

Who Needs Access?

1. Set **minimum** access levels for **effective** productivity

1. Restrict access (admin, user, guest, 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*

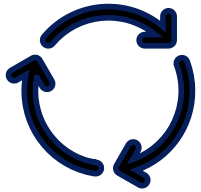
- Network/physical segmentation
  - *Insecure devices on the network (i.e., IoT devices)*

- Third-party access
  - *Attack delivered through a third-party action (deliberate or unintentional spread of a virus)*

STEP 2

Update Your Defenses

- Apply s**ecurity** u**pdates (patches**)
  - Issued by manufacturers and developers to fix coding loopholes/vulnerabilities
- Encrypt data at rest

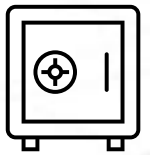


Set to Auto Update

+

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

+



Encrypt your data

STEP 3

Beyond Simple Passwords

GLOBAL CYBER ALLIANCE

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

- Computing power has increased over time, while size and cost has decreased
  - The Apple iPhone 5 (2012) has over 2.7 times the processing power of a Cray 2 supercomputer (1985) that is 1.2m high, 1.4m diameter and weighs nearly 2,500kg!

How Passwords Can Be Cracked

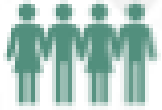
- Using computing power to cycle through different combinations
  - Increasing computing power and AI are making this quicker and cheaper
  - ***Use long passwords or passphrases, numbers, and special characters***

- Using known common passwords and available lists
  - ***Use memorable words/passwords but not common ones or ones that might be associated with you***

- Once they are in one account they will try the same username/password elsewhere
  - ***Use a different password for each account***

- Phishing with links to a ‘lookalike’ website so you enter your log in details
  - ***Be wary of all unsolicited emails/approaches, use a known good address to access accounts from your browser***

How Passwords Can Be Cracked



- Social engineering tricks people into revealing passwords
  - ***Never give out your password, or parts of it, to anyone.***

- By manual guessing i.e., names, dates of birth, family and pet names….
  - ***What does the web and social media say about you?***
  - ***Steer clear of Personally Identifiable Information (PII) in passwords***

- They can be brought on the dark web
  - ***Change your password if your details may have been included in a data breach***

- Passwords can be intercepted as they are transmitted over a network
  - ***Check for https green padlock***
  - ***Avoid public WiFi***
  - ****https DOES NOT infer a genuine website just an encrypted link***

Two-Factor Authentication (2FA)

GLOBAL CYBER ALLIANCE

Multi-Factor Authentication/Two-Step Verification MFA/2SV

Provides increased levels of protection against compromise

Something you know:

- A password

AND something you have:

- A token (Google Authenticator, Okta, RSA)

- A verification code sent to your phone

- A fingerprint or face (biometrics)

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

STEP 4

Prevent Phishing and Malware

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 related to work you’re doing
- They may have called you or your nonprofit/charity 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

What Harm Could a Phishing Email Do?

GLOBAL CYBER ALLIANCE

- 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 or text

Check via a known good media - Report it!

Ransomware

Ransomware: malware that blocks access to a system, device, files, or steals sensitive data until a ransom is paid - usually in cryptocurrency (i.e., bitcoin).

Examples of ransomware attacks:

- HSE: 54 public hospitals – May 2021
- Evide: impacting 140 charities, nonprofits, councils – Mar 2023
- Extern: Apr 2024

Prevent with patching, auto-updates, AV, strong access controls…

Recover with regular, external backups, incident response plan…

While it may be tempting to pay the ransom, the general advice is NOT TO

Backups Are Critical to Business Continuity

Downtime can seriously impact your productivity and sustainability.

How much would it cost if you:

- Could not use IT for a day?

- Lost customer data?

- Lost an important business deal?

- Were held to ransom?

These could happen for several reasons - hard disc failure, human error, equipment stolen, cyber-attack, accidental damage, etc.

Having backups is critical to being able to quickly recover and resume operations!

STEP 5

Backup and Recover

- Know your data – impact of loss
- On and off-line backups
- Have a plan

STEP 6

Protect Your Email and Reputation

- DMARC

What If Someone Sent An E-mail Pretending To Be You ….

- They copied your logo and email format

- But changed your bank details on the appeal/email
  - or your telephone number in the signature

- Or your website address behind a ‘CLICK HERE’ to donate button

- Or instructed a staff member to set up a new payment?

How would you know they had done it?

How would your donors/supporters know it wasn’t you?

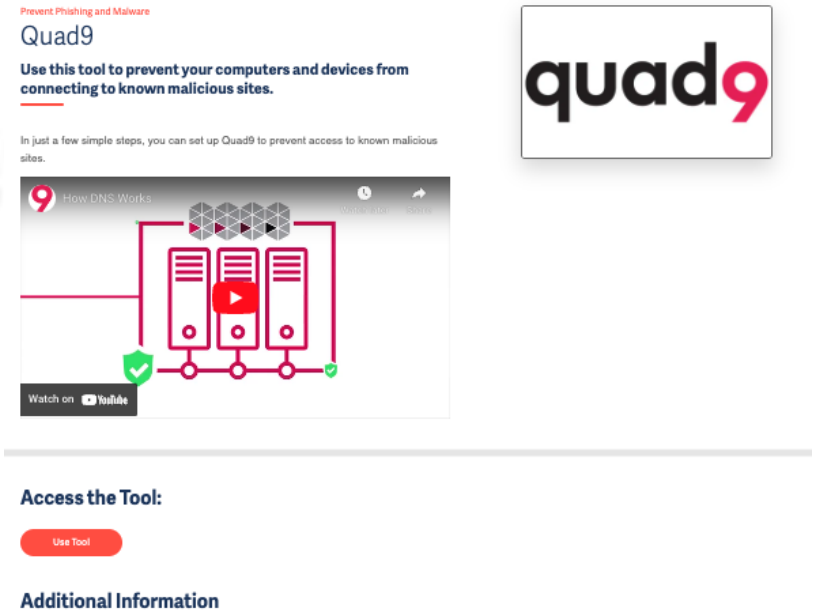
Would your internal staff know what to do?

STEP 7

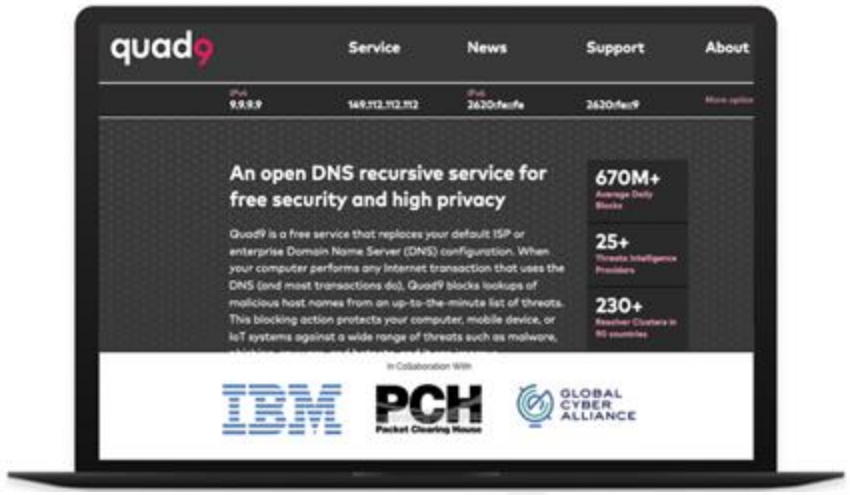
Communicate Securely

- Keep your communications private
- Consider using digital signatures
- Use of encrypted channels and VPN for email, texts, voice calls, internet access
- Use of some apps may be banned in certain jurisdictions

Example Tool: Quad9



Blocks access to known bad websites



- **Quad9**: Checks IP address against threat intelligence feeds. Blocks if known bad.
- Average **670+ million blocks** per day. **Easy** to set up

GCA Cybersecurity Toolkit for Mission-Based Organizations

Free

Straight forward

Global

Private

Sponsored by Public Interest Registry

In partnership with Global Cyber Alliance

Essential cyber hygiene will significantly reduce your risk of attack

https://gcatoolkit.org/mission-based-orgs/

Additional Useful Resources

- An Garda Síochána
  - https://www.garda.ie/en/crime/cyber-crime/
  - https://www.garda.ie/en/crime/fraud/
- National Cyber Security Centre NCSC
  - https://www.ncsc.gov.ie/guidance/
  - https://www.ncsc.gov.ie/pdfs/Cyber_Vitals_Checklist.pdf
- European Cybersecurity Month *#ThinkB4UClick*
  - https://cybersecuritymonth.eu/countries/ireland