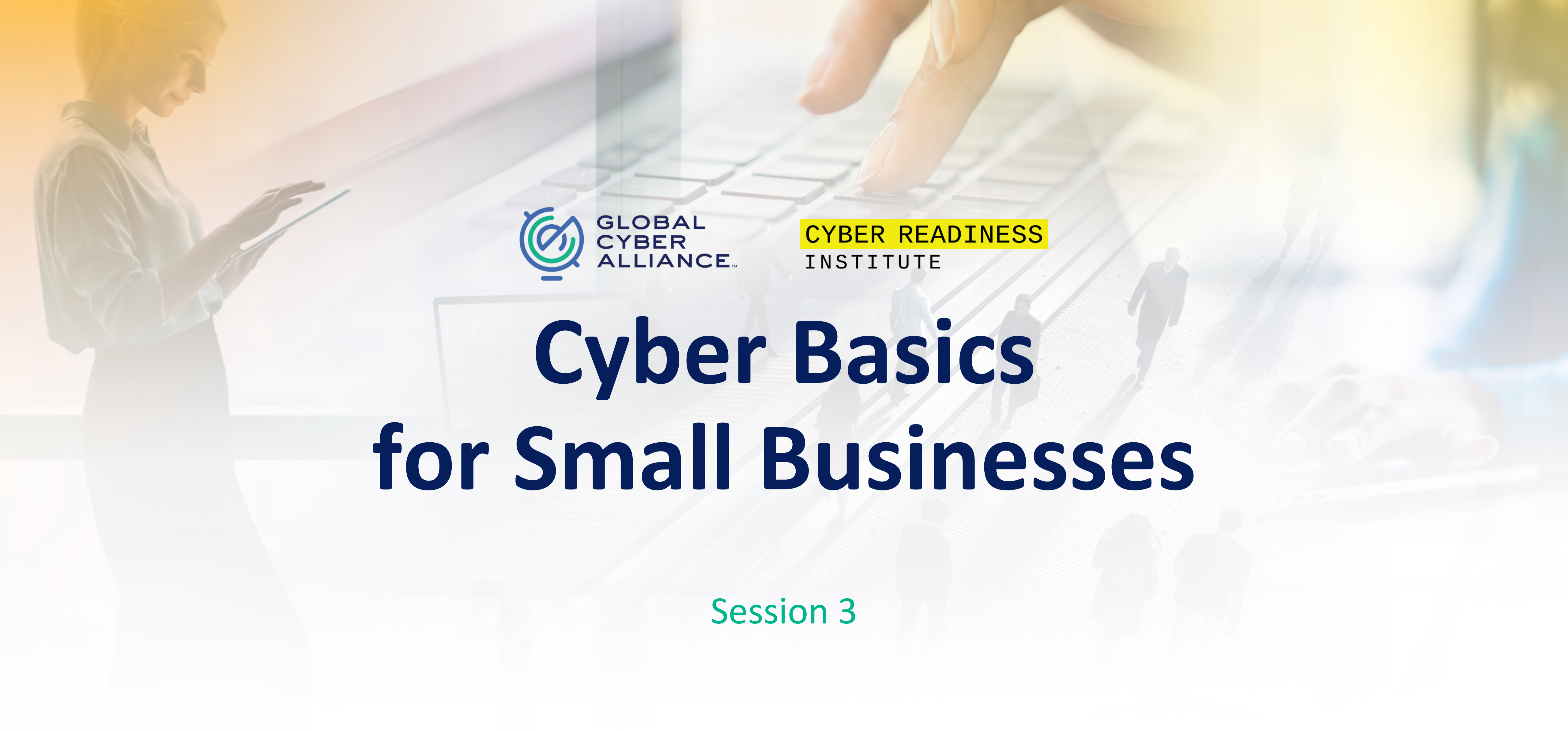


GLOBAL CYBER ALLIANCE

CYBER READINESS INSTITUTE

Cyber Basics for Small Businesses

Session 3

Today’s Agenda

GLOBAL CYBER ALLIANCE | CYBER READINESS INSTITUTE

Backup and Recover

- Why backups are important for your business
- Different types of backups
- Recovering from Ransomware

Protect Your Email and Reputation

- DMARC
  - Know what it stands for
  - Why it’s important
  - What attacks it mitigates
- Check your domain to see if DMARC is enabled

Week 2 Refresher

Prevent Phishing and Malware

- 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

Backup and Recover

What Are Backups?

- Copies of key information or data that are stored separate to your device
- If an incident occurs you can restore data and get back to business.

- The average global cost of a data breach is **$3.92 million (USD) -** *Ponemon 2019 Cost of a Data Breach*
- Headlines focus on large businesses
- Smaller businesses are statistically more likely to suffer an attack
- *ICO fined Bible Society £100,000 after a breach*
  1. Criminals do not care
  2. You have an obligation

Backups Are Critical to Business Continuity

Downtime can seriously impact your company's productivity and profitability.

How much would it cost if you:

- Could not use IT for a day?
- Could not access customer files?
- Lost an important proposal?
- Were held to ransom?

These could happen for a number of reasons - hard disc failure, human error, equipment stolen, cyber-attack, accidental damage.

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

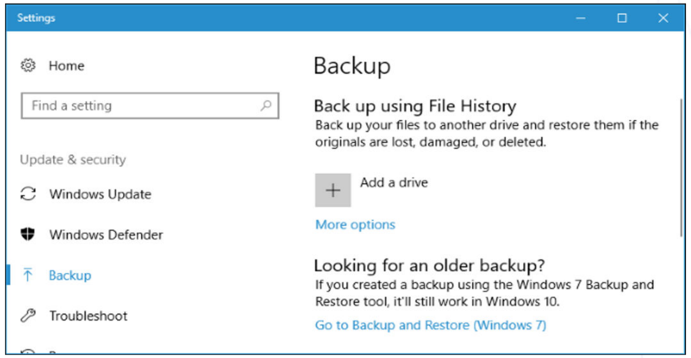
Types of Backups

Offline backups

- Local and offline (external hard drive, USB drive, memory card, etc.)
- Schedule, disconnect and keep in a separate location.

PROS:

- Most machines come with automatic backup software
- Backing up can be cheap and fast
- You don’t need an internet connection



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

CONS:

- You have to remember to plug in your device
- Separate but accessible location in case of an emergency
- Limited by your external drive space

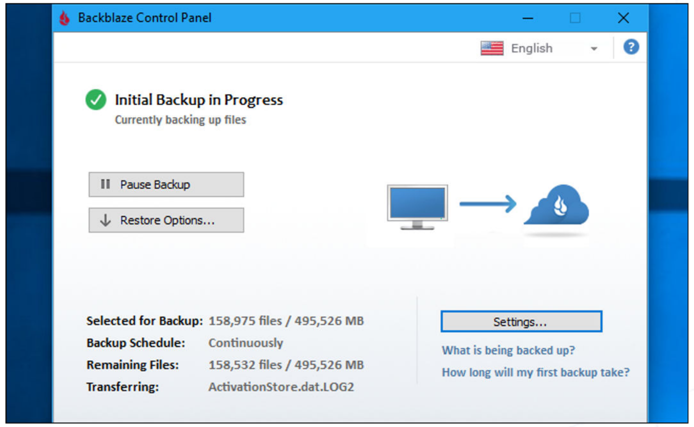
Types of Backups

Online Backups

Online or cloud backups make copies of your important data and store them offsite on secure servers ‘in the cloud.’

PROS:

- Online backup protects you against data loss from hard drive failure, theft, natural disasters...
- Can set schedule to automatically back up



Backblaze Control Panel

English

Initial Backup in Progress
Currently backing up files

Selected for Backup: 158,975 files / 495,526 MB
Backup Schedule: Continuously
Remaining Files: 158,532 files / 495,526 MB
Transferring: ActivationStore.dat.LOG2

What is being backed up?
How long will my first backup take?

CONS:

- Must be connected to the internet
- Rental cost based on size
- Malware could get backed up

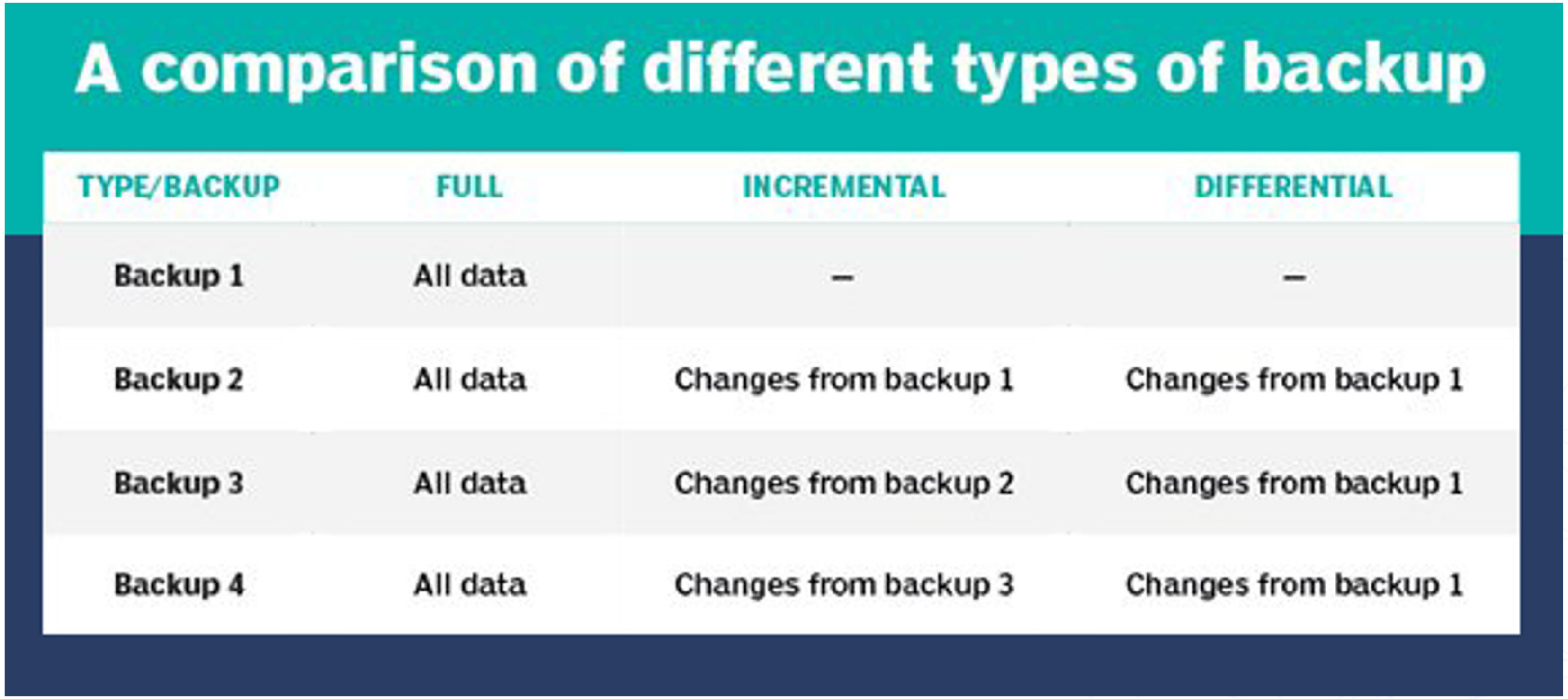
Types of Backups

Full Backups

- The most basic and complete backup

Incremental Backups

- Copying only data that has changed since the last backup



A comparison of different types of backup

TYPE/BACKUP	FULL	INCREMENTAL	DIFFERENTIAL
Backup 1	All data	–	–
Backup 2	All data	Changes from backup 1	Changes from backup 1
Backup 3	All data	Changes from backup 2	Changes from backup 1
Backup 4	All data	Changes from backup 3	Changes from backup 1

Differential Backups

- This will initially copy all data changed from the previous backup (akin to Incremental backups).
- Will continue to copy all data changed since the previous full backup.

Ransomware and Backups

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

Examples of ransomware attacks:

- NHS affected by ransomware May 2017
- TravelEx affected by ransomware Jan 2020

Prevent with patching, auto-updates and AV
Recover with regular and external backups

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

Backup and Recover

- Categorize your data
  - Consider impact of loss
- Create a sensible policy that's right for your organization
  - Automatic and scheduled
  - Test this plan regularly

Protect Your Email and Reputation

Phishing

MikeKeefe2004
IT'S OK, HON... IT'S JUST THE BANK ASKING ME TO VERIFY SOME CREDIT CARD INFO.
PHISHING SEASON

- Could lead to
  - Ransomware or other malware
  - Fraud (false wire transfer requests)
  - Theft of PII
- Why is it successful?
  - Difficulty in determining if message came from legitimate source
  - From\Sender address is spoofed

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 invoice
- And changed your telephone number in the signature
- Or instructed a staff member to set up a new payment

How would you know they had done it?

How would your customer/supplier know it wasn't you?

Would your internal staff know what to do?

Do you have processes in place to address BEC…

Business Email Compromise (BEC):

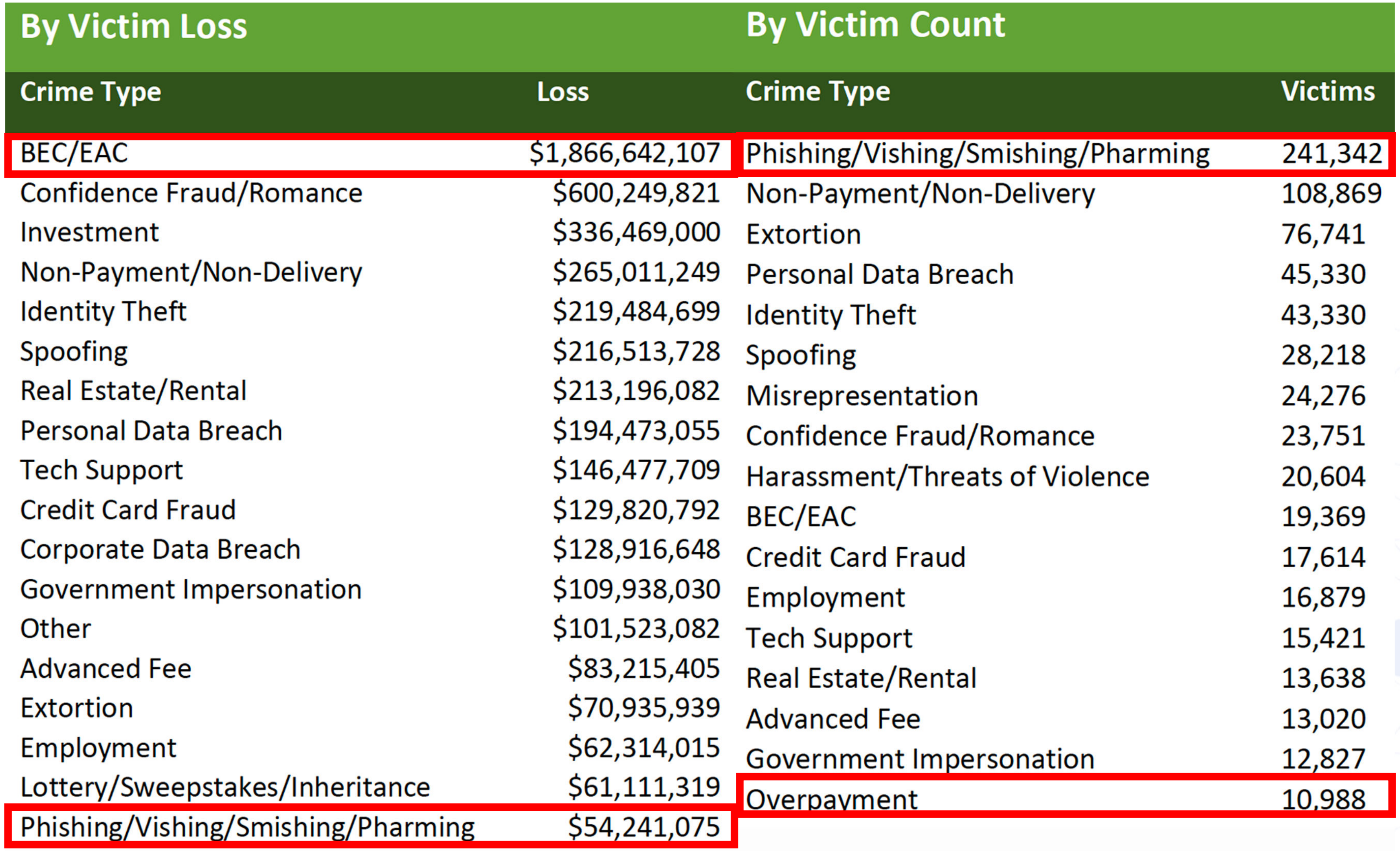
- Also known as Email Account Compromise (EAC)
- Scams could consist of:
  - Spoofing an email account or website
  - Sending spear phishing emails
  - Using malware

Business Email Compromise (BEC) in $$$

City - $1.04 million
City - $1.73 million
City - $800K
Religious Institution - $1.75 million

(source: *bleepingcomputer.com*)

FBI 2020 Internet Crime Report



By Victim Loss		By Victim Count	
Crime Type	Loss	Crime Type	Victims
BEC/EAC	$1,866,642,107	Phishing/Vishing/Smishing/Pharming	241,342
Confidence Fraud/Romance	$600,249,821	Non-Payment/Non-Delivery	108,869
Investment	$336,469,000	Extortion	76,741
Non-Payment/Non-Delivery	$265,011,249	Personal Data Breach	45,330
Identity Theft	$219,484,699	Identity Theft	43,330
Spoofing	$216,513,728	Spoofing	28,218
Real Estate/Rental	$213,196,082	Misrepresentation	24,276
Personal Data Breach	$194,473,055	Confidence Fraud/Romance	23,751
Tech Support	$146,477,709	Harassment/Threats of Violence	20,604
Credit Card Fraud	$129,820,792	BEC/EAC	19,369
Corporate Data Breach	$128,916,648	Credit Card Fraud	17,614
Government Impersonation	$109,938,030	Employment	16,879
Other	$101,523,082	Tech Support	15,421
Advanced Fee	$83,215,405	Real Estate/Rental	13,638
Extortion	$70,935,939	Advanced Fee	13,020
Employment	$62,314,015	Government Impersonation	12,827
Lottery/Sweepstakes/Inheritance	$61,111,319	Overpayment	10,988
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Types of Spoofing

- Display Name Spoofing - *“**Company** <person@yahoo.com>”*
  - *Hover over the display name to check the actual address*
- Domain Name Spoofing - *“Company <person**@company.com**>”*
  - *Use DMARC*
- Lookalike Domain Spoofing - *“Company <person@co**rn**pany.com>”*
  - *Check the email address carefully*

SOLUTION:

DMARC

A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)
It’s like an identity check for your organization’s domain name.

What is DMARC?

A DMARC policy allows a sender to indicate that their messages are protected, and tells a receiver what to do if one of the authentication methods passes or fails – such as send the message or junk/reject the message.

Benefits of Using DMARC

- **Offers** brand protection
  - Prevents an impersonator ‘pretending to be you’ in an email
- **Prevents** you from receiving an email from an imposter
  - More than 80% of consumer inboxes are protected with DMARC verification
- Improves **Deliverability**
- **Provides** an insight into attempts to spam, phish, or spear-phish using your organization's email domain
- Both the sender and receiver must have it
- If you and your customer/supplier use DMARC, ***both*** are PROTECTED from email domain spoofing - **so please spread the word**

What Happens to the Messages?

- Depends on the policy setting:
  - **None** - reports possible suspicious mail messages, but all mail is sent to inbox
  - **Quarantine** - fails authentication; message is sent to spam/junk folder
  - **Reject** - fails authentication; message is dropped and not delivered at all

- Best practice is to start at **None** and *gradually* move to **Reject**

CRI Additional Resources

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

GCA Cybersecurity Toolkit for Small Business

https://gcatoolkit.org/smallbusiness/

- Backing up and Recover
- Protect Your Email and Reputation

GCA Learning Portal

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

- Protecting Your Business Data with Backups
- Protect Against Email Spoofs & Phishing

GCA Community Forum

http://community.globalcyberalliance.org/

Cyber Basics Resources

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

Email Authentication for Better Email Security

DEFEND & DELIVER

DMARC BOOTCAMP

MAY 5, 2021

Sign-up here: https://gca.globalcyberalliance.org/bootcamp-registration-may-2021

Q & A

Summary

Know What You Have and Update Your Defenses

- Create and maintain an Inventory
- Keep software patched to the latest revision (Set to auto-update)
- Keep staff and third-party access under constant review

Beyond Simple Passwords

- Ensure all your accounts use strong and different (unique) passwords
    - Remember those lesser used devices
- Enable MFA/2FA for all your accounts (where MFA/2FA is supported)

Prevent Phishing and Malware

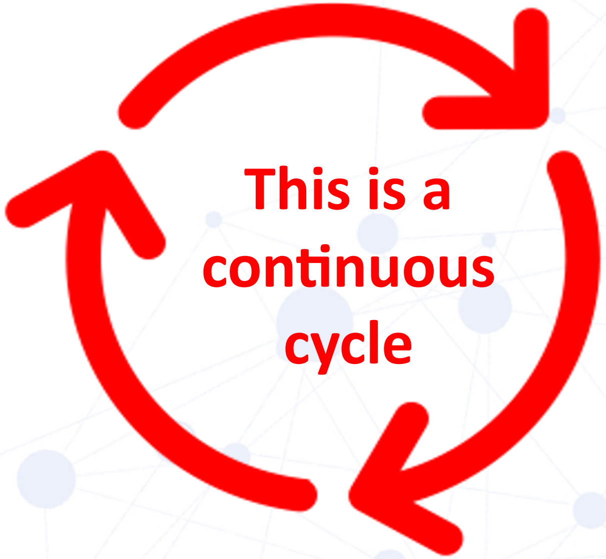
- Anti-virus on all devices
- Regular Staff Awareness Training
- Use DNS Filtering

Backup and Recover

- Categorize your data
- Create a sensible policy that's right for your organization
    - Automatic and scheduled
    - Test this plan regularly

Protect Your Email and Reputation

- Use DMARC for your organization's email



This is a continuous cycle

Thank You!

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

Copyright Global Cyber Alliance 2021