TECHIMPACT®

CYBER SECURITY BASICS

THANKS TO OUR SPONSORS!

Training Series Underwritten By:

MVP HEALTH CARE

Sponsored By:

Hudson Valley Funders Network

nycon

New York Council of Nonprofits, Inc.

Unleashing the Power of Nonprofits


WE’RE A NONPROFIT ON A MISSION
TO USE TECHNOLOGY TO BETTER
SERVE THE WORLD.

TECHIMPACT®

We do this by delivering tech services, education, and training that help nonprofits and communities thrive.

NONPROFIT TECH SERVICES:

- Managed IT Support
- Cloud Migration
- Cyber Security & Compliance
- Data Systems Support
- Strategic Consulting & Planning
- Machine Learning & AI
- Community Integrated Design

NONPROFIT EDUCATION & TRAINING:

- Nonprofit Technology Reports
- Consumer Guides to software
- Technology Assessments
- Workbooks & Articles
- Online Training Courses
- Free Webinars

WORKFORCE DEVELOPMENT:

ITWorks & CXWorks:
Free IT and Customer Experience training programs

PunchCode:
12-week immersive programming bootcamp

TECHIMPACT®

LINDA WIDDOP

Managing Director of Client Solutions, linda@techimpact.org

I manage all aspects of client relations for Tech Impact including educating nonprofits about technology solutions. I work with local, regional and national partners to provide the nonprofit community with increased knowledge of technology through speaking engagements.

I am an obsessed birder who loves to travel and engage in citizen science projects that help inform environmental protection actions.

DAVID ADKINS

NYCON Board Member

I've served in technology leadership positions for organizations like NYSERDA (New York State Energy Research & Development Authority), the New York State Bar Association and New York State United Teachers. I am currently a member of Hudson Valley Community College's School of Business Advisory Committee and teach graduate level courses at the University of Maryland, University of Dayton, and SUNY Albany in Information Technology, Cybersecurity, and Data Analytics.

AGENDA

1. Introduction to Cyber Security Principles
2. Vulnerabilities – Threats, Actors and Vectors
3. Costs of Data Breaches
4. User Attacks
5. Device Attacks
6. Remote Work Threats
7. Securing Your Data & Staying Safe

INTRODUCTION TO CYBER SECURITY PRINCIPLES

WHAT IS CYBER SECURITY?

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked.

This environment includes users, networks, devices, software, processes, information (in storage or transit), applications, services, and systems that can be connected directly or indirectly to networks.

NONPROFITS ARE ESPECIALLY AT RISK

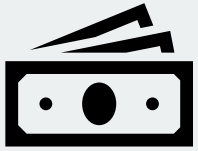
- Often have tons of sensitive data
- Stepping stones into bigger targets
- Too busy with meaningful work to divert time/energy/money to security
- Some staff are not computer savvy

VULNERABILITIES – THREATS, ACTORS & VECTORS

ASSETS – WHAT ARE THE CYBER CRIMINALS AFTER?

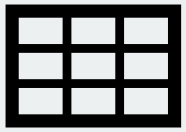
Access

Usually they want *access* to computers and servers in order to launch scams and attacks on other organizations



Money

Nothing shocking here – looking for quick cash transfers



Data

Standard information like medical records, credit numbers have commodity pricing information on the black market. $x/record

Information

If they are against your mission, they might want damaging information or internal communications, but this is extremely unlikely.

ACTORS - WHO WANTS THOSE ASSETS?

- Cyber Criminals
- Staff
- Adversaries

CYBER CRIMINALS

- External Attackers stealing email account credentials for spam or fraud
- External Attackers repurposing servers, computers, or networking equipment for botnets or fraud
- External Attackers phishing to make money
- Protecting against these is a matter of making it harder for the attacker to get in. They often go after someone else

INTERNAL STAFF

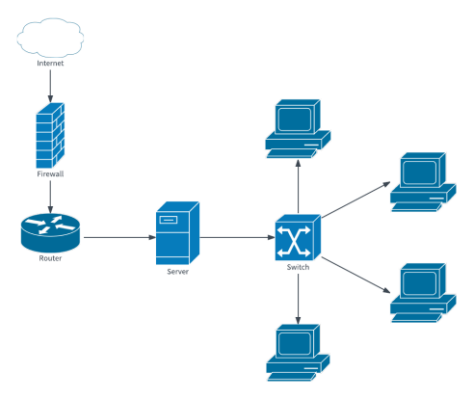
- Careless with data and credentials
- Stealing information
- Coverup
- Installing inappropriate software
- Falling for Phishing Scams

A recent Verizon study indicates that internal users account for 80% of all security breaches!

ADVERSARIES

Adversaries are people actively opposed to your mission who want to disrupt your ability to deliver programs or damage your reputation.

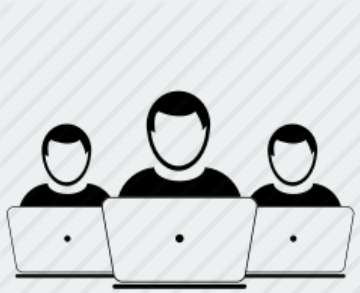
THREAT VECTORS: (AKA HOW DO THEY GET IN?)



Network Penetration

Phishing Scams

Lost / Stolen
Malware / Virus



User Error

CYBER SECURITY THREAT VECTORS

Device Security

Ensure our devices are safe and that their loss will not endanger the organization

Data Loss Controls

Ensure that sensitive information doesn't intentionally or accidentally get put somewhere unsafe, or sent to someone who shouldn't have it

Item-level Encryption

Provide extra protection to specific highly sensitive information to prevent sharing

Account Security

Ensure that people have only the level of access they really need, and that we know who is accessing what

Malware Controls

Minimize the exposure of our devices to risky software and websites, and ensure that active protections are in place to defend against new and unknown malware

Network Controls

Monitor our networks and protect them from direct penetration attempts

HOW CONCERNED SHOULD YOU BE?

TECHIMPACT®

COSTS OF DATA BREACHES

COST OF DATA BREACH

- Tangible Costs
- Intangible Costs
- Insurance Coverage

COST OF A DATA BREACH: ACTUAL COSTS

Estimates an average of $146 per lost record, and $11.45 million average total cost. Costs include:

- system recovery
- data restoration
- legal guidance
- breach notification
- forensics
- credit monitoring

Source: Ponemon Institute 2020 Cost of Data Breach Study

COST OF A DATA BREACH: INTANGIBLE COSTS

The lost trust that nonprofits experience from donors, volunteers and the community can affect

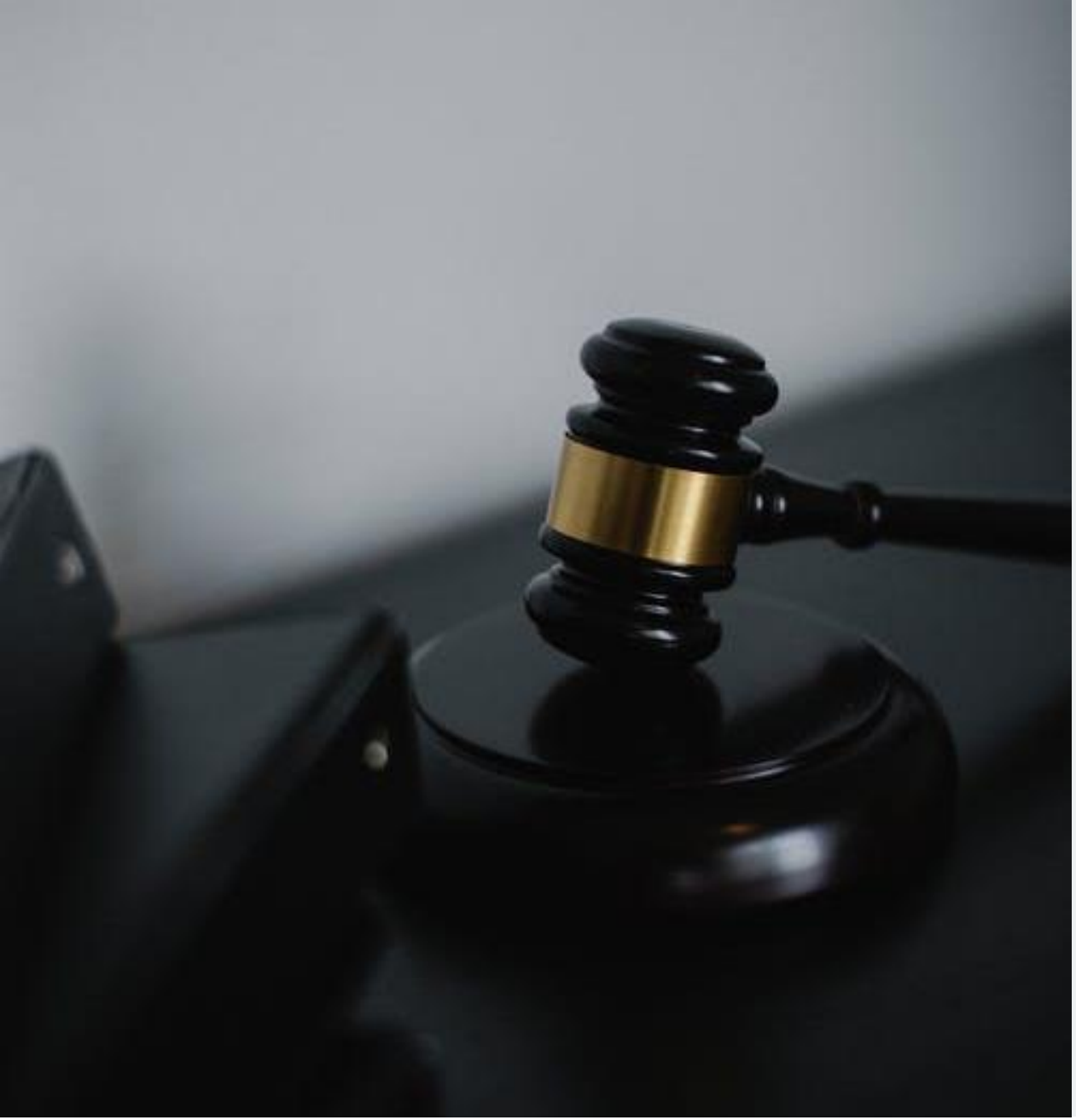
- fundraising activities
- volunteer engagement
- partnerships with other organizations

Source: Ponemon Institute 2020 Cost of Data Breach Study

DIFFERENT LEVELS OF DATA BREACH INSURANCE COVERAGE

First-party data breach insurance provisions include:

- Data breach investigation costs
- Hardware and software damage costs
- Fines incurred by lost data
- Lost revenue



DIFFERENT LEVELS OF DATA BREACH INSURANCE COVERAGE

Third-party data breach insurance provisions include:

- Lawsuits from individuals due to data loss
- Fees incurred for aiding individuals in the event of data loss

IT'S NOT "IF", IT'S "WHEN"

Security Breaches are going to happen even if your organization has taken steps to secure the environment and train users.

- Act Quickly – contact your IT professional at the first hint of trouble
- Follow the Plan – know what to do, how to communicate
- Recover Losses – invoke your insurance plan

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

USER ATTACKS

OBVIOUS PHISH

From: 2020-03-20 23:09 <Techimpact@eu.ficamdif.com>
Sent: Friday, March 20, 2020 11:09 AM
To: Patrick Callihan <patrick@techimpact.org>
Subject: FW:Review on Corona Virus Update for Techimpact on 2020-03-20 23:09
Importance: High

Office 365 ***Coronavirus Review***

Recent Update on Coronavirus disease (COVID-19)
COVID-19 ID: #NIPH

CASE ID: Coronavirus
EMMERGENCY NO: 911 - 112
EMAIL ID: EDCARN@ who.int

REVIEW NOW;:

NOT-SO-OBVIOUS PHISHING

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before **[[current_date_1]]**.

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

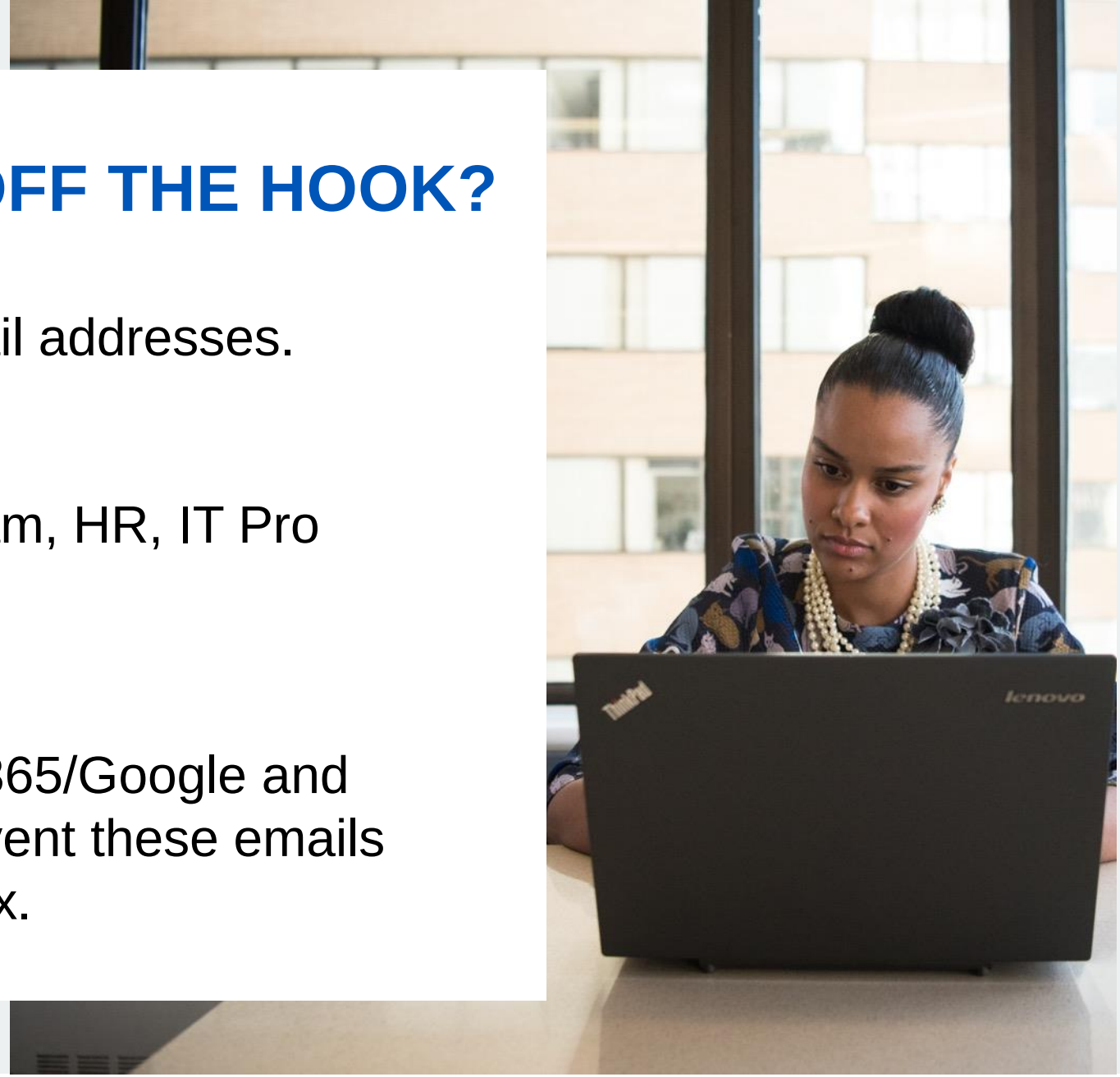
Regards,
Human Resources

HOW CAN FISHES STAY OFF THE HOOK?

Only open email from known email addresses.
(check the email address twice!)

Check with your management team, HR, IT Pro before clicking any links.
(use phone or chat to verify)

Your IT Pro can configure Office 365/Google and some other email systems to prevent these emails from coming through to your Inbox.



USER SECURITY

Device Security

Ensure our devices are safe and that their loss will not endanger the organization

Data Loss Controls

Ensure that sensitive information doesn't intentionally or accidentally get put somewhere unsafe, or sent to someone who shouldn't have it

Item-level Encryption

Provide extra protection to specific highly sensitive information to prevent sharing

Account Security

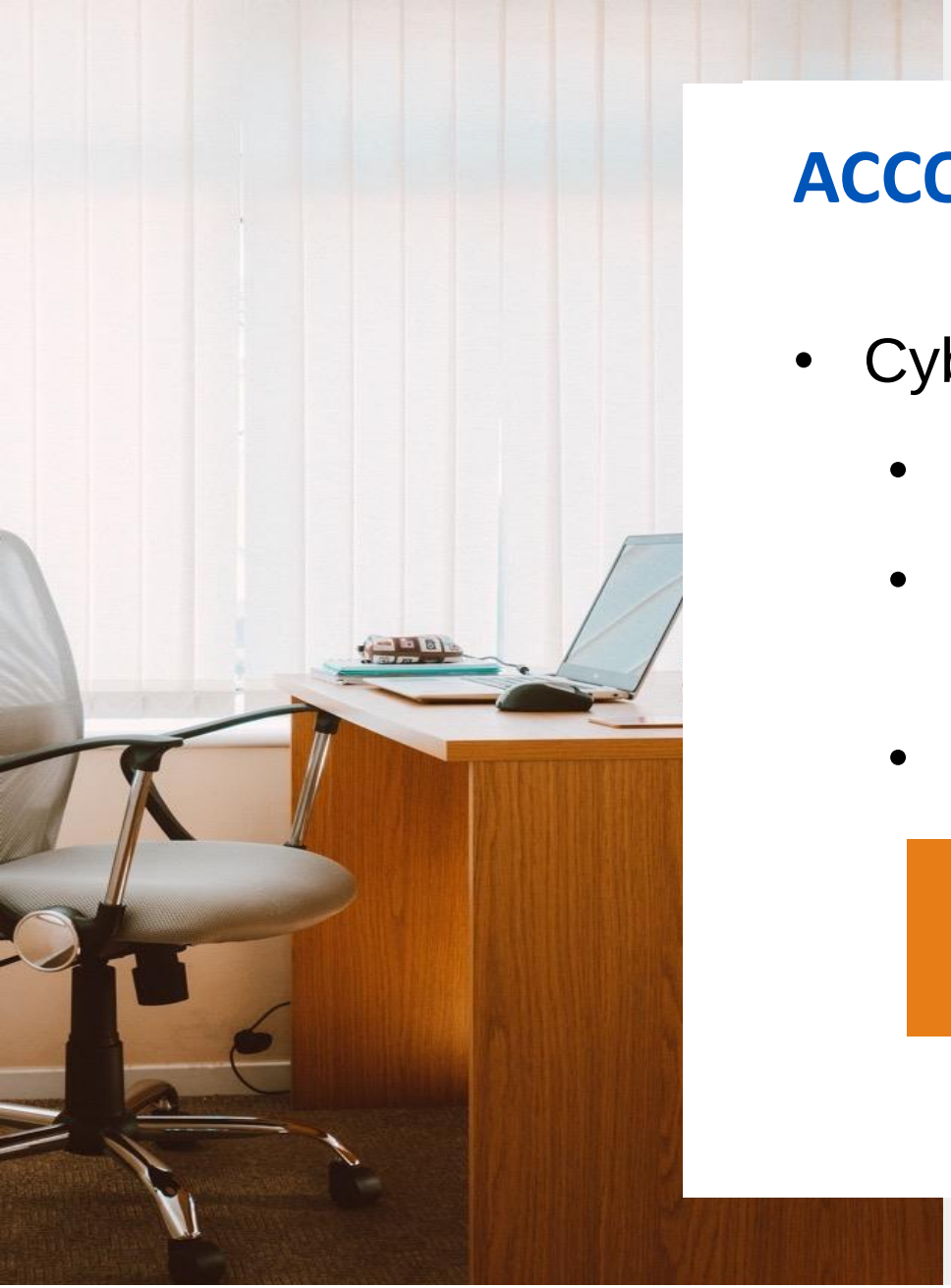
Ensure that people have only the level of access they really need, and that we know who is accessing what

Malware Controls

Minimize the exposure of our devices to risky software and websites, and ensure that active protections are in place to defend against new and unknown malware

Network Controls

Monitor our networks and protect them from direct penetration attempts



ACCOUNT SECURITY

- Cyber Criminals gain access to your credentials
  - Steal money from your account(s)
  - Use credentials to unlock other systems (admin rights)
  - Spoof your email to continue attacks on others

Internal Users account for up to 80% of all cyber breaches

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

DEVICE ATTACKS

DEVICE SECURITY

Device Security

Ensure our devices are safe and that their loss will not endanger the organization

Account Security

Ensure that people have only the level of access they really need, and that we know who is accessing what

Data Loss Controls

Ensure that sensitive information doesn't intentionally or accidentally get put somewhere unsafe, or sent to someone who shouldn't have it

Malware Controls

Minimize the exposure of our devices to risky software and websites, and ensure that active protections are in place to defend against new and unknown malware

Item-level Encrypt-ion

Provide extra protection to specific highly sensitive information to prevent sharing

Network Controls

Monitor our networks and protect them from direct penetration attempts

ORGANIZATION-OWNED

- Updated operating system, desktop apps
- Updates, AV/AM maintained by IT Pro
- User authentication managed by AD/AzureAD or other

vs.

PERSONAL COMPUTERS

- Home version of operating system, desktop apps
- Probable bloatware/trial apps
- Updates, AV/AM managed manually by user. May not be best of breed
- Computer access open to all family members
  - Hard to protect against family downloading malware/viruses
  - Org data can be accessed by family members

BRING YOUR OWN DEVICE (BYOD) POLICIES

Personal devices present risk to the organization:

Outdated, Home version of OS and applications

Lack of / outdated AV

No user authentication / weak passwords

Mobile devices lost or stolen

MAM

Mobile Application Management

Control Of Applications

- Best suited for personally owned devices
- Can apply security settings to applications:
  - Restrict actions
  - Set authentication policies
  - Selective wiping of organizational data

MDM

Mobile Device Management

Control Of Full Device

- Best suited for organizational owned devices
- Can set security parameters:
  - Requiring PIN or Multi-Factor Authentication
  - Remote Wipe & Password Reset

DEVICE SECURITY

Cyber Criminals gain access to your computer/device

- Gain access to your accounts through keylogging
- Launch attacks against others through your computer
- Encrypt your device for ransom

Anti-virus and Anti-malware software are a must!

REMOTE WORK THREATS

CYBER SECURITY THREAT VECTORS

Device Security

Ensure our devices are safe and that their loss will not endanger the organization

Data Loss Controls

Ensure that sensitive information doesn't intentionally or accidentally get put somewhere unsafe, or sent to someone who shouldn't have it

Item-level Encrypt-ion

Provide extra protection to specific highly sensitive information to prevent sharing

Account Security

Ensure that people have only the level of access they really need, and that we know who is accessing what

Malware Controls

Minimize the exposure of our devices to risky software and websites, and ensure that active protections are in place to defend against new and unknown malware

Network Controls

Monitor our networks and protect them from direct penetration attempts

TECHIMPACT®

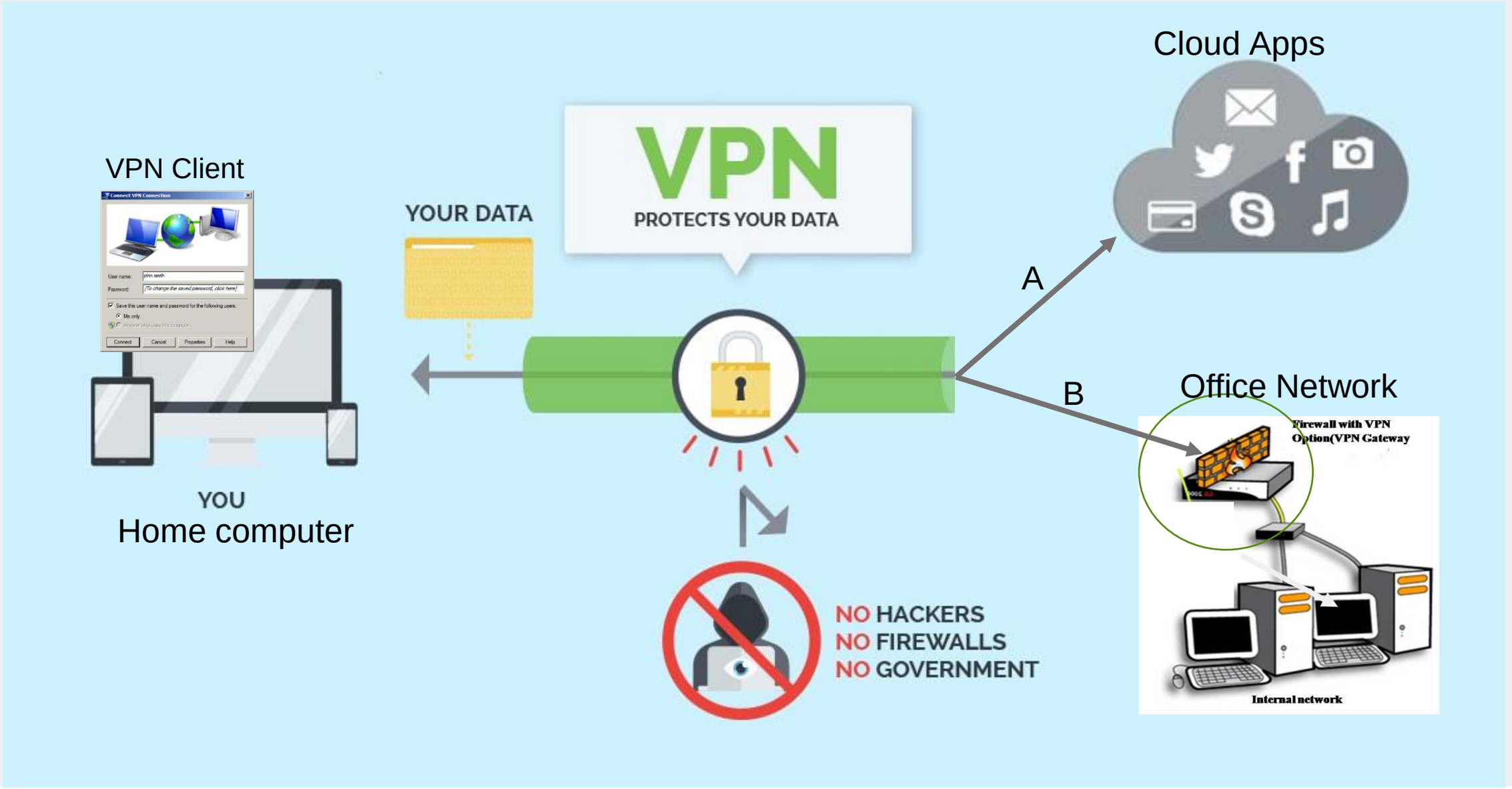
CLOUD COMPUTING

- Cloud vendor provides secure platform
- Browser access is secured via HTTPS protocol
- Data is stored in secure data center
- Accessible from any device

VPNS AND REMOTE DESKTOP PROTOCOLS

VPNs and Remote Desktop Protocols create a “tunnel” for your data to travel through securely.

VIRTUAL PRIVATE NETWORK (VPN)



TECHIMPACT®

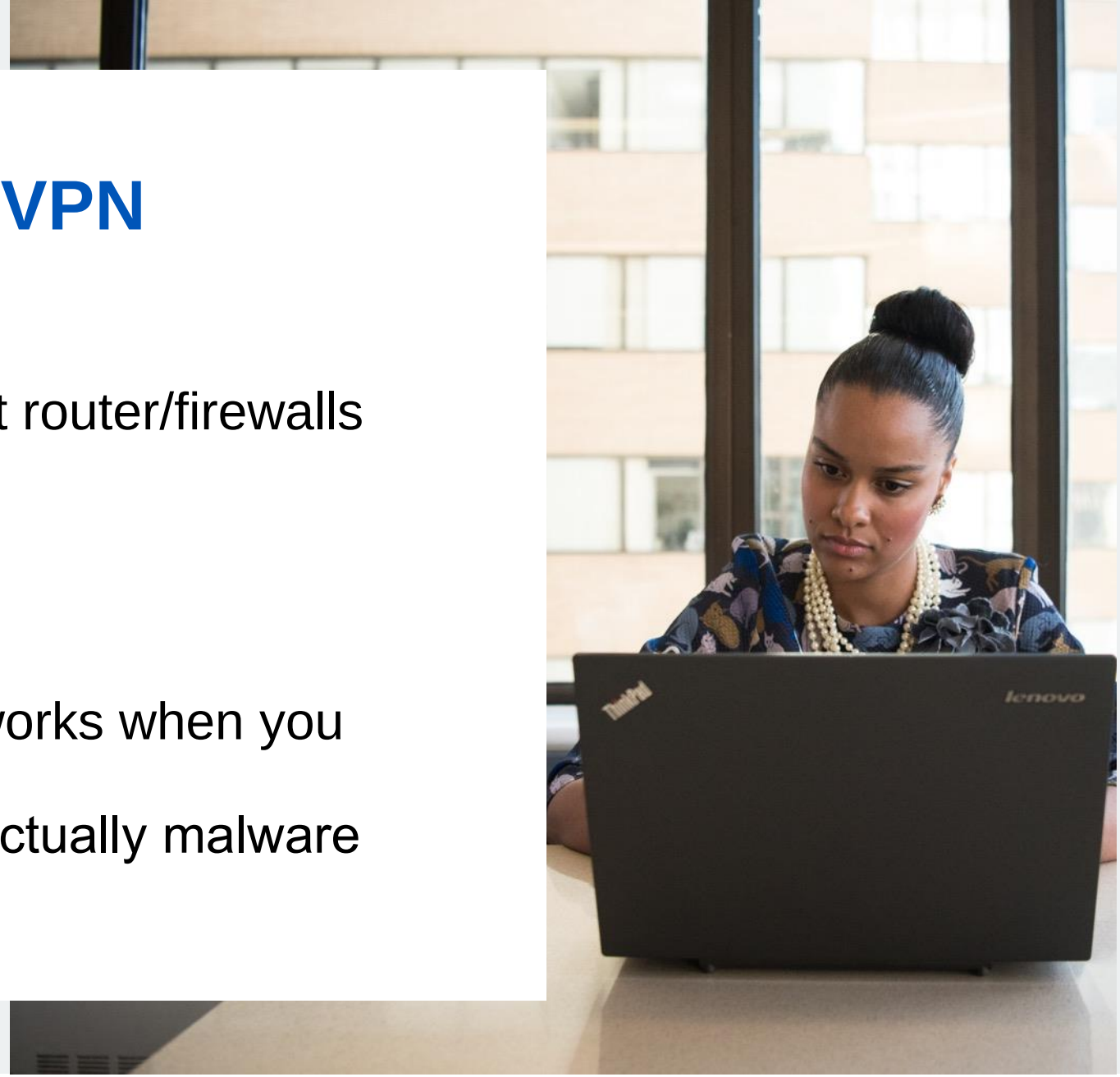
PROS AND CONS FOR VPN

VPN Pros:

- VPN function is built into most router/firewalls

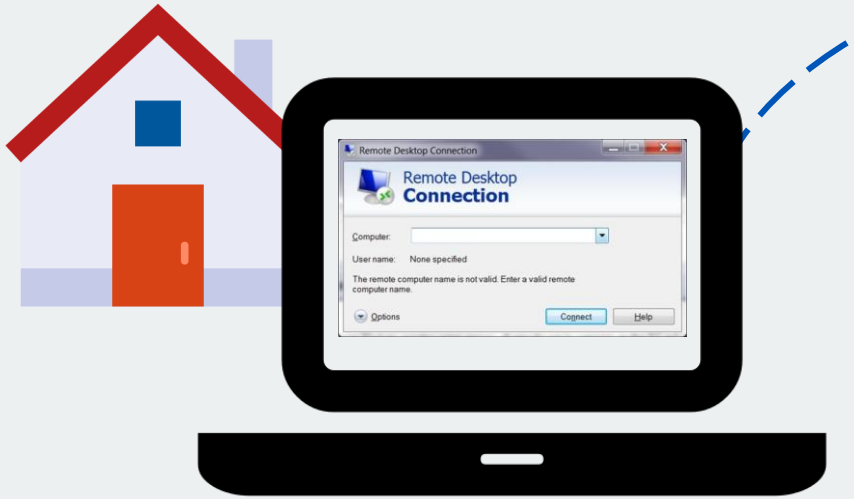
VPN Cons:

- Requires additional licensing
- Connection is finicky (never works when you need it most)
- Many “free” VPN clients are actually malware



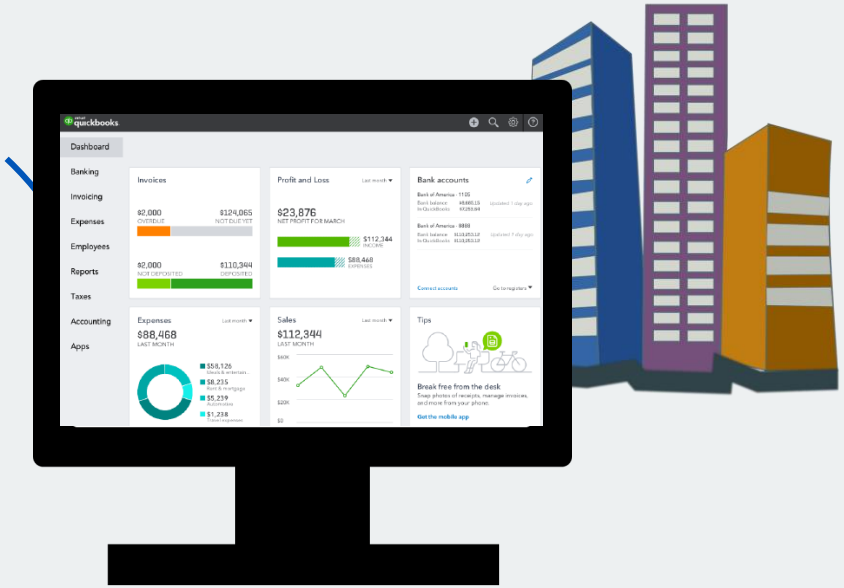
REMOTE DESKTOP CONNECTION (RDC)

Remote staff computer



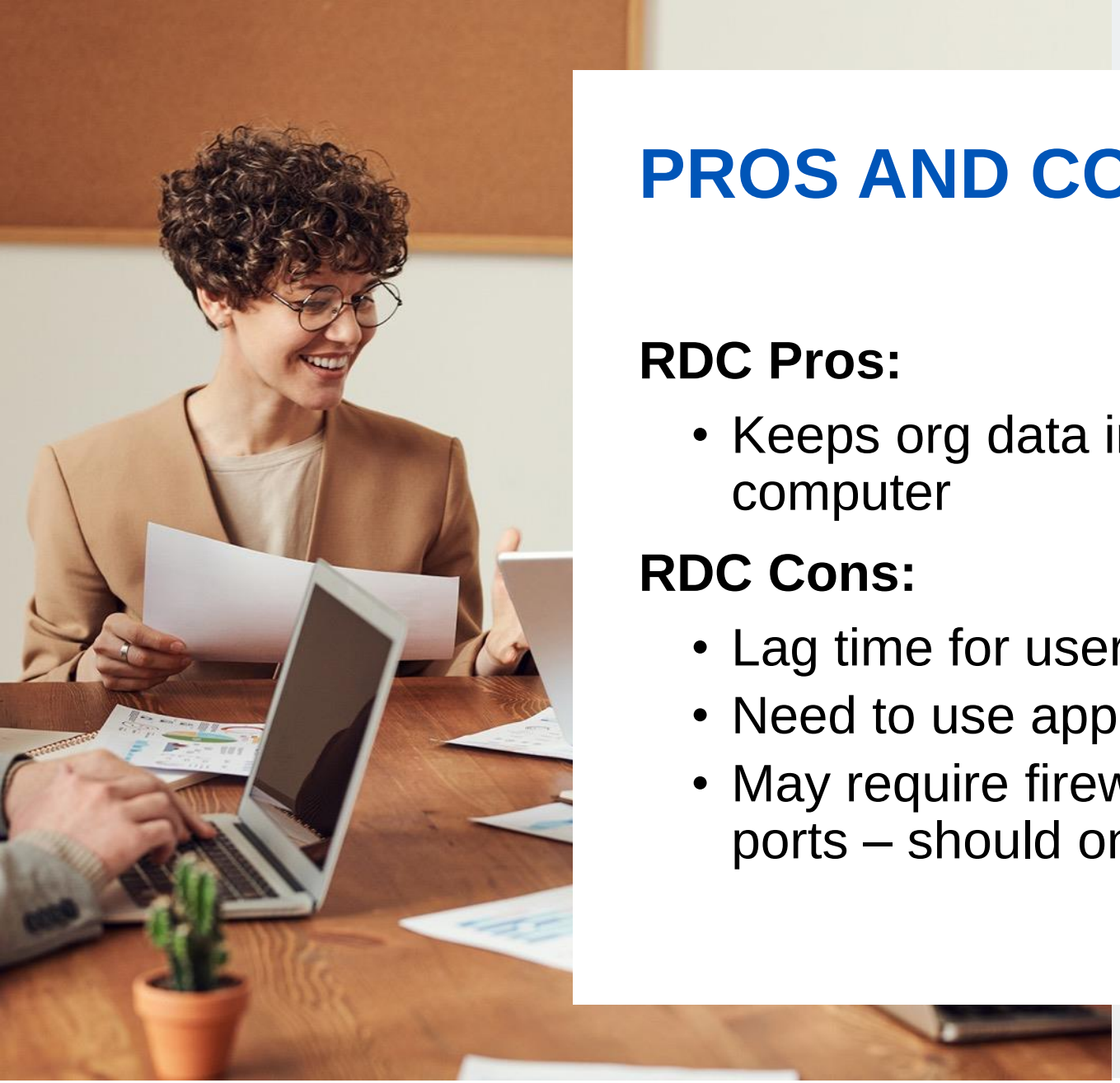
Use this mouse/keyboard

Computer in office



…and this computer will do all the work and send back a live image of the desktop.

TECHIMPACT®



PROS AND CONS FOR RDC

RDC Pros:

- Keeps org data in the office and not on the home computer

RDC Cons:

- Lag time for users depending on Internet speed
- Need to use approved RDC client like TeamViewer
- May require firewall setting changes that could open ports – should only be completed by IT Pro deves

VPN AND REMOTE DESKTOP RESOURCES

VPN:
Meraki
Sonicwall

Remote Desktop:

Microsoft RDC
TeamViewer
GoToMyPC
LogMeIn

Average commercial price is $40-50 per year per computer.

Don’t use a free version.

TECHIMPACT®

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

SECURING YOUR DATA & STAYING SAFE

YOUR GOAL IS NOT TO FIX EVERYTHING

Perfect security isn’t possible.

Trying to implement perfect security is a waste of resources that hamstrings and frustrates your team and actually makes you less safe.

The goal here is balance.

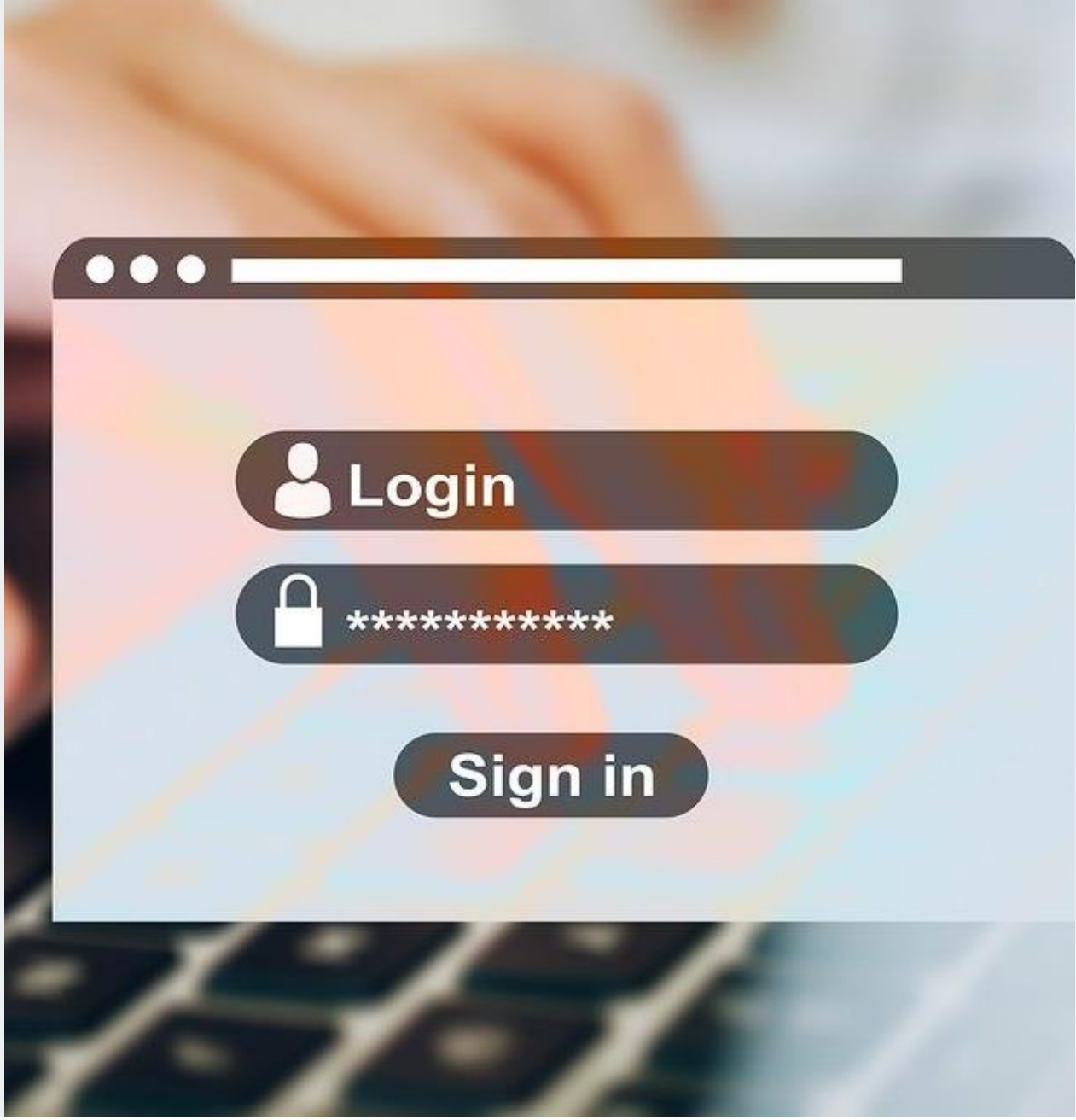
HOW CAN NONPROFIT WORKERS STAY SAFE?

1. Never click a link in an email unless you know what it is AND who it is from.
2. Only get your news from trusted sources such as .gov websites.
3. Don’t open ANYTHING from social media.
4. Don’t download a mobile app for COVID-19.
5. When in doubt, don’t click the link. If it’s legit, the sender will contact you again.
6. When in doubt, ask your management team for approval.

USER CREDENTIAL CYBERSECURITY TIPS

Ensure password best practices

- Use strong passwords
- Never save organization passwords in your browser
- Use a password manager



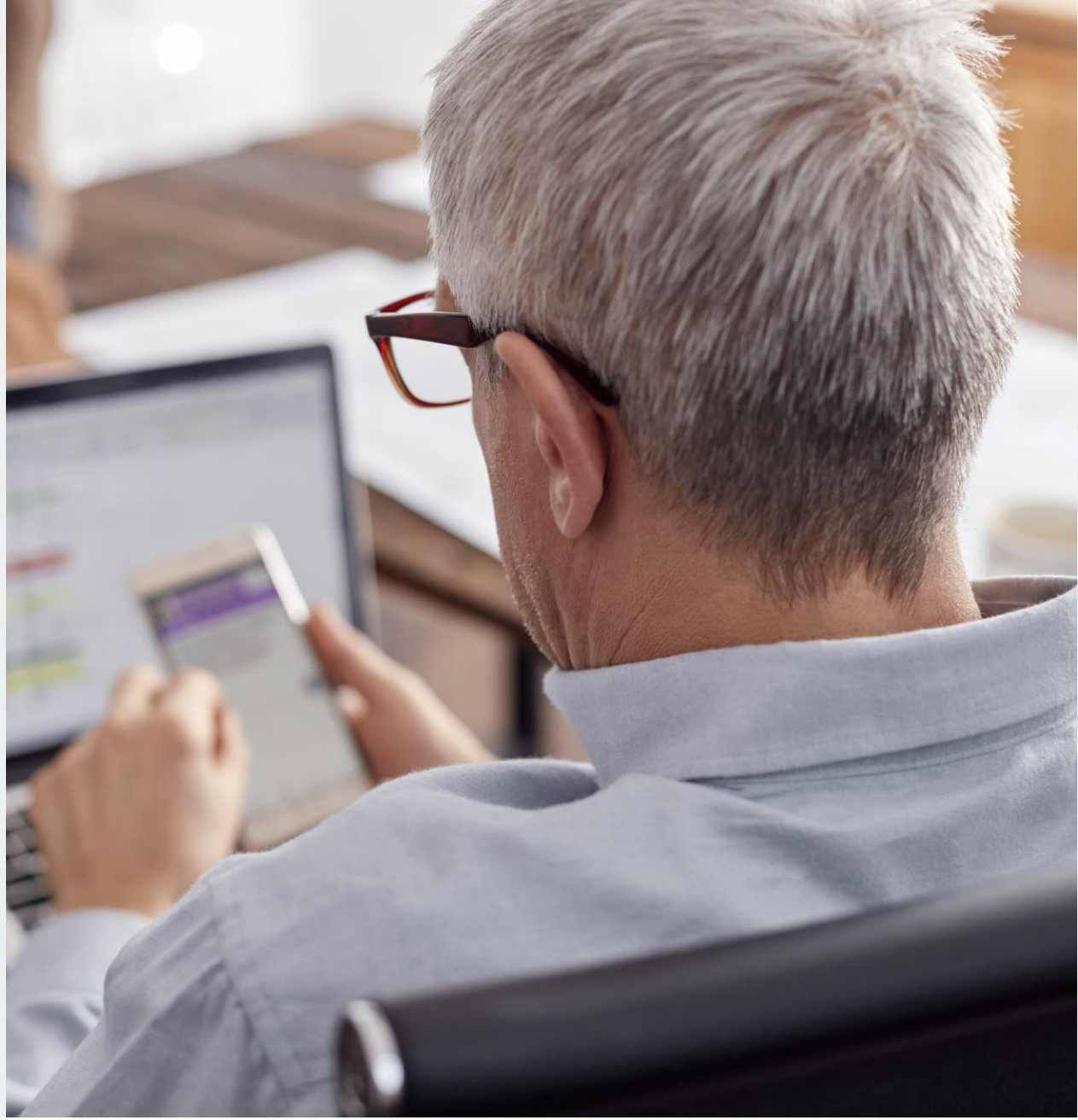
TECHIMPACT®

USER CREDENTIAL CYBERSECURITY TIPS

Multi-factor Authentication (MFA) protects against compromised user credentials.

Single Sign-On (SSO) allows access to cloud systems with one password that is managed by the organization.

- O365
- OKTA



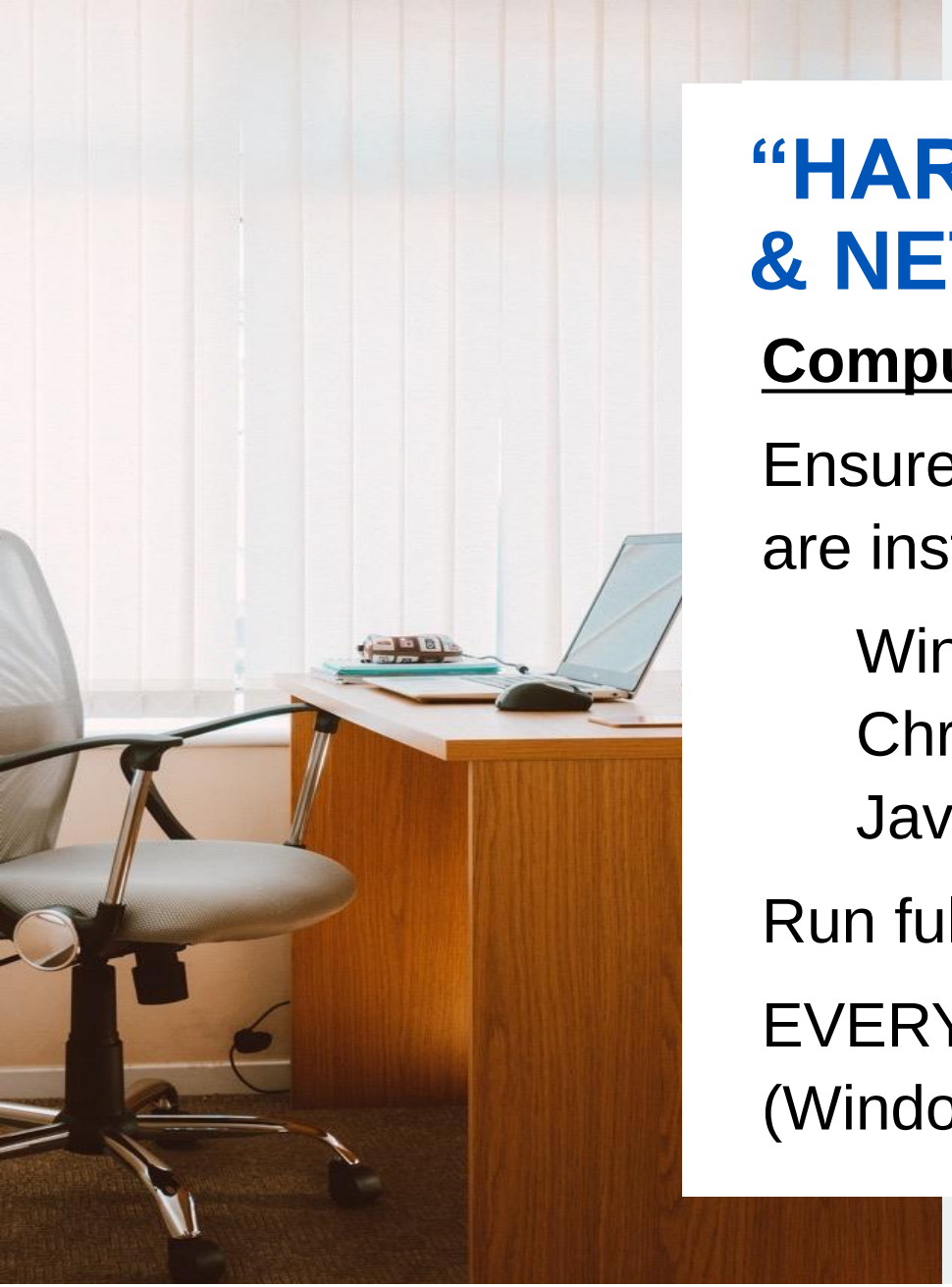
TECHIMPACT®

TARGETED ATTACKS

Advanced adversaries are those that specifically target you and have the technical means to pull it off. Usually their aim is espionage and/or damaging your reputation.

Protecting yourself is possible but difficult. You need to be hardened, not just harder. That probably means compromises for your staff.

Protecting against government actors is even harder because you often can’t use cloud-based services.



“HARDEN” HOME COMPUTERS & NETWORKS

Computer Hardware

Ensure all available updates are installed each day:

Windows, Firefox / Chrome, Adobe Reader, Java, Zoom, GoToMeeting

Run fully up-to-date antivirus

EVERY DAY
(Windows Defender is fine)

Network Security

Home WiFi Networks

- Set up a password,
- Change default SSID and admin credentials

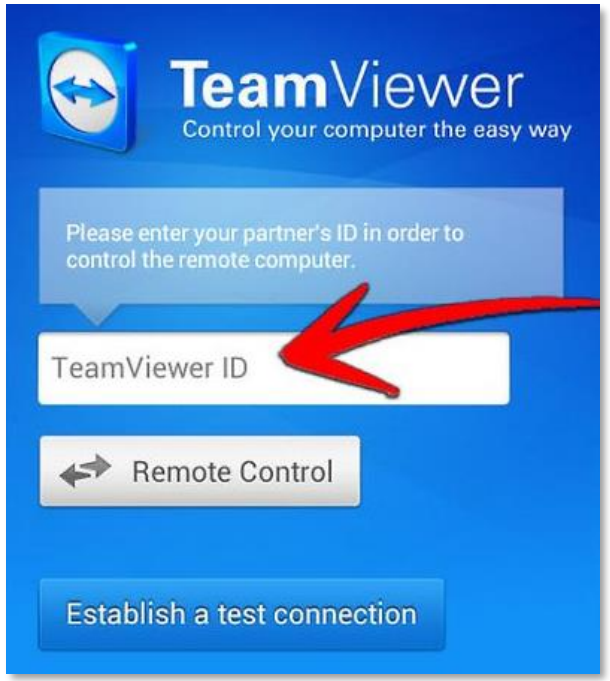
Use an approved VPN or remote desktop connection.

VPN BEST PRACTICES

- Use IT Pro approved VPN client connected to your network's firewall
  - Requires licensing and configuration
- Do not use free VPN apps
- Only use the VPN tunnel when you need to connect, then disconnect to allow others access

REMOTE DESKTOP BEST PRACTICES

- Use IT Pro approved RDC client to connect to your computer
- Your office computer must be turned on – and power saver mode disabled. Client installed and configured in office first
- Also use a VPN client to encrypt data over RDP
- May need to close port 3389 on home router – ask your IT Pro
- Connect only when needed, then disconnect
- Your home computer MUST have appropriate updates/security/AV etc



TECHIMPACT®

REMOTE WORKER BEST PRACTICES

- Make sure staff can identify phishing emails.
- Use strong passwords for all systems.
- Enable Multi-Factor Authentication (MFA) on ALL systems.
- Harden home networks.
- Do not allow data to be stored on home computers.
- Create a policy and train staff on the policy - can be done in an all-staff webinar, etc.

TECHIMPACT®

EDUCATION AND BEST PRACTICES

Staff Training:

- KnowBe4 Cyber Security Training
  - Self-serve
  - Managed
- Policies
  - Review and revise all computer policies

KnowBe4
Human error. Conquered.

TECHIMPACT®

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

THANK YOU!

Connect with Linda Widdop at linda@techimpact.org.