WEBINAR

Remote Work and Cybersecurity: Supporting Employees Amid a Pandemic

March 18, 2020

Eric Vanderburg
Vice President, Cybersecurity
TCDI

Bogdan Salamakha
Senior Cybersecurity Engineer
TCDI

Frank Yako
CIO – Director of Strategic Initiatives
ASMGi

AGENDA

01 Remote Work Considerations

02 Common Cybersecurity Attacks & Strategies

03 Supporting Remote Employees

Remote Work Considerations

01

Remote Work Considerations

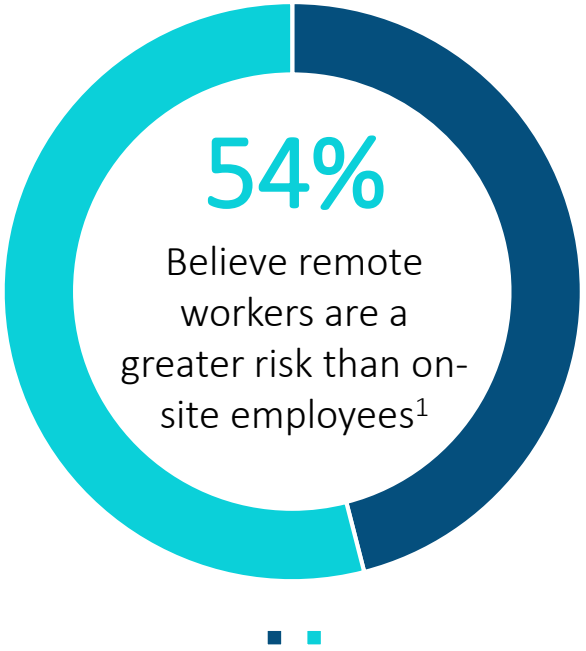
Is your network equipped to handle an influx of remote workers logging in?

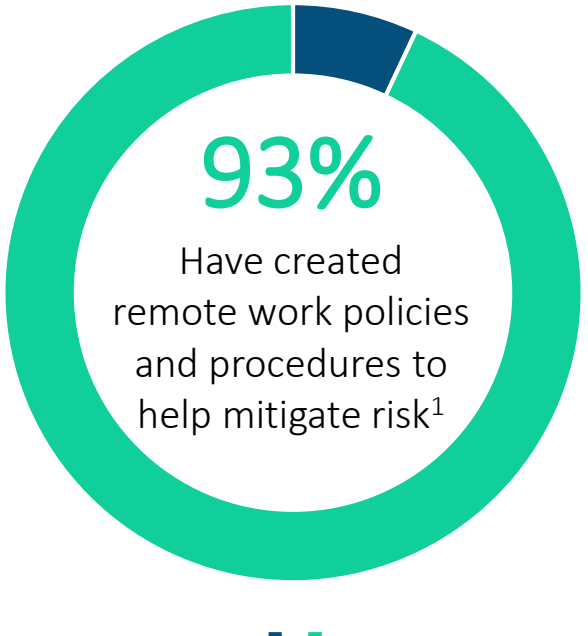
4.7 Million

employees in the US work remotely[2]

= **1.4%**

of the population



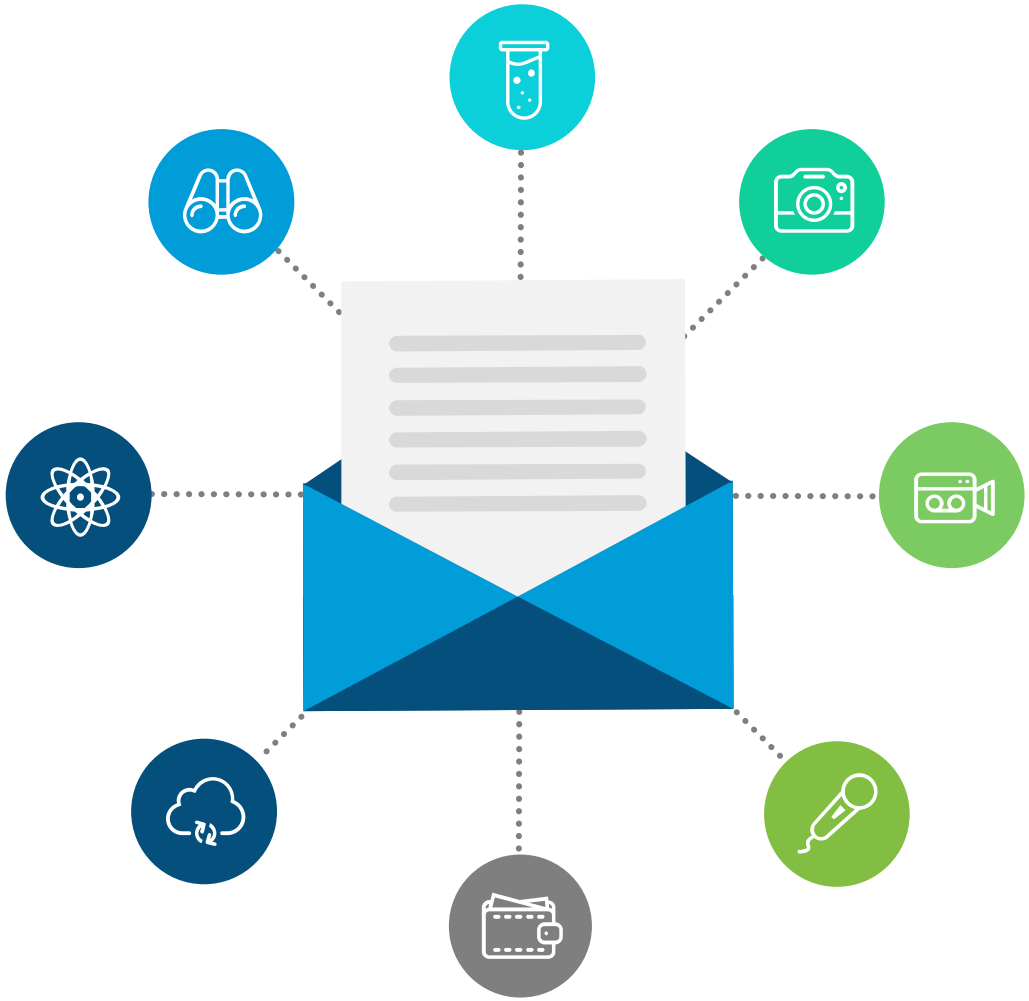


1 https://openvpn.net/remote-workforce-cybersecurity-quick-poll/
2 https://amtrustfinancial.com/blog/small-business/remote-workers-and-cyber-liability

Common Cybersecurity Attacks & Strategies

What is Phishing?

- May contain viruses, spyware, inappropriate material or “scams” or fraudulent schemes
- Tricks users into revealing sensitive information, such as passwords, SSN, Bank Account numbers, etc. including for fraudulent or identity theft purposes
- Don’t disclose passwords, SSN, Bank Account numbers or other sensitive information via email, text, social media or phone



Business Email Compromise Starts with a Phish

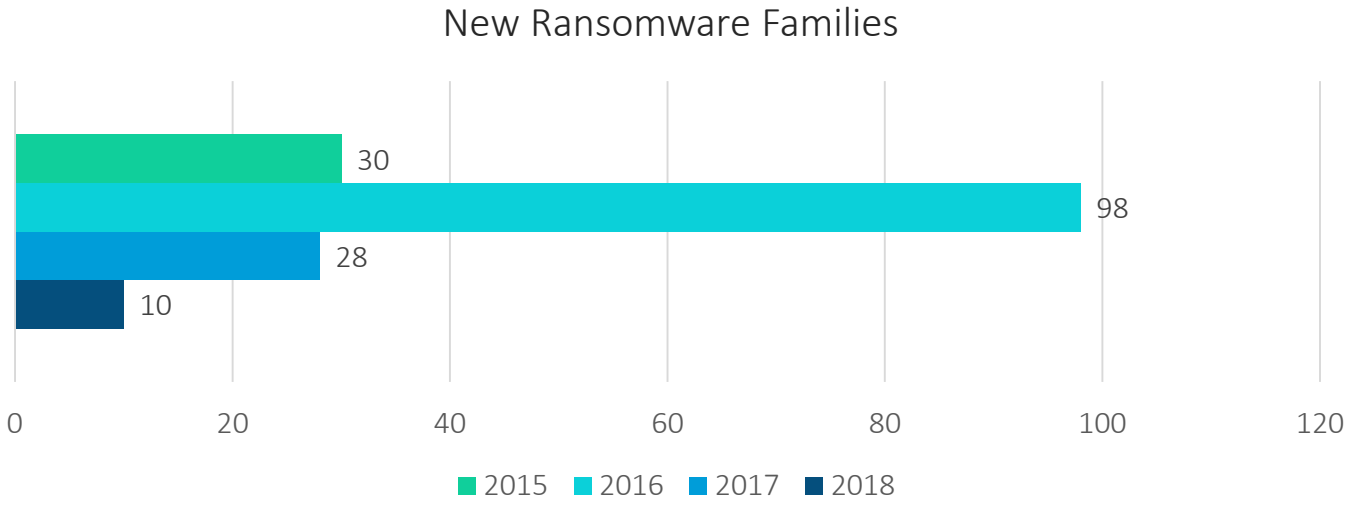
Targets well-placed individuals — those who control financial accounts — at both large and small organizations with very targeted spear-phishing attacks.

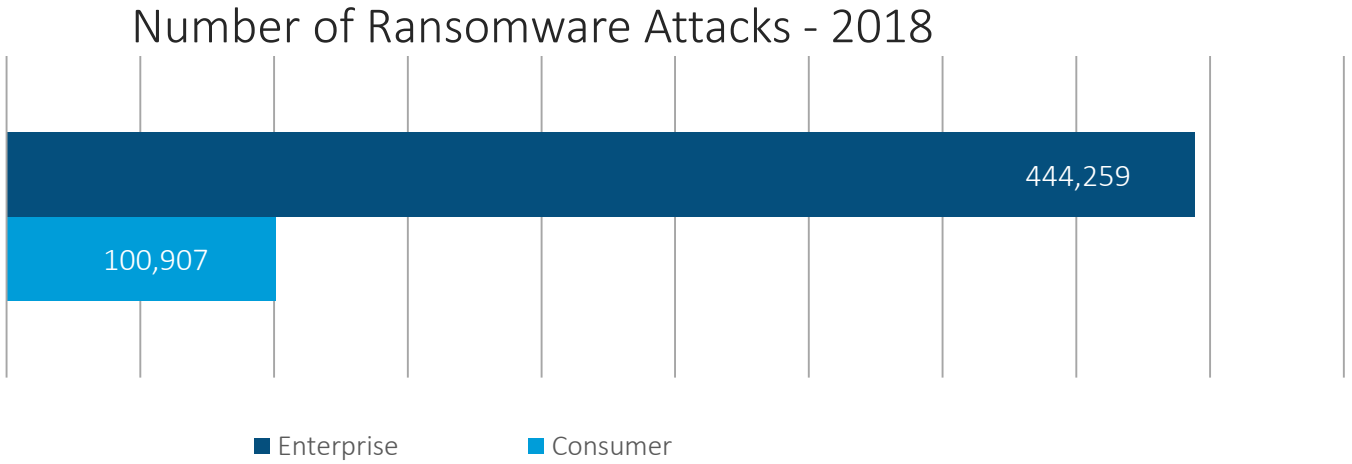
Targets also include junior employees that report to leadership that receive email impersonating the CEO or CFO.

Comes in various forms including bogus invoice, CEO fraud, account compromise, attorney impersonation, and data theft.

Overall, in 2018 the FBI received more than 351k reported scams with losses exceeding $2.7 billion.

BEC attacks per targeted organization increased 476% year-over-year in the last quarter of 2018.





Ransomware

A study conducted by Symantec tracked different families and variants of ransomware through 2018.

Ransomware as a Whole

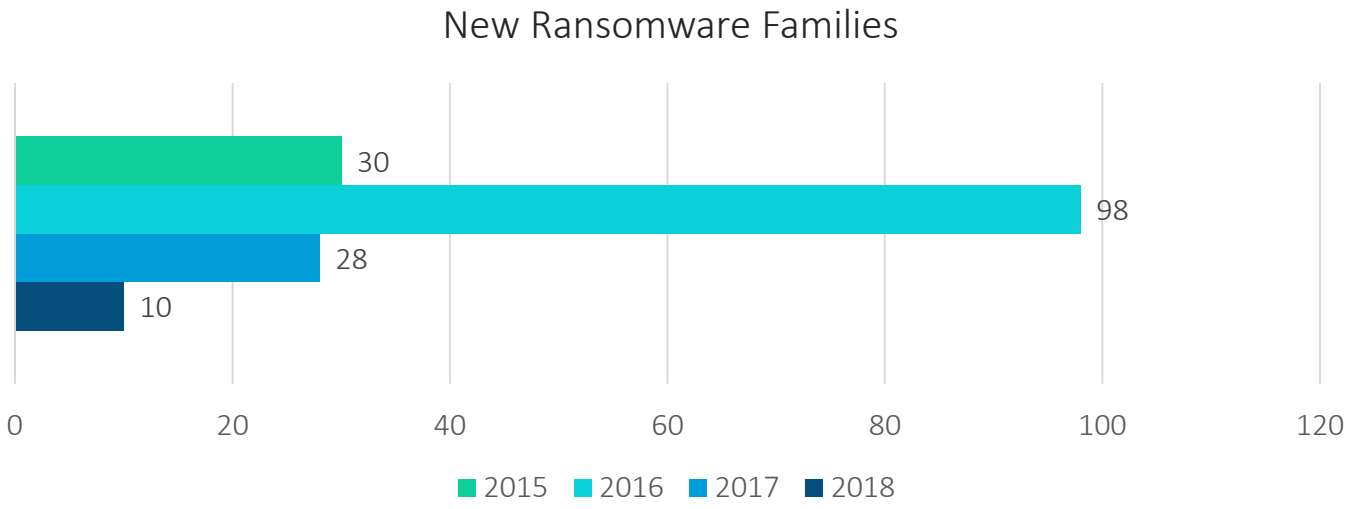
The number of new ransomware families fell in 2018, and there was a decrease in the overall number of ransomware infections.

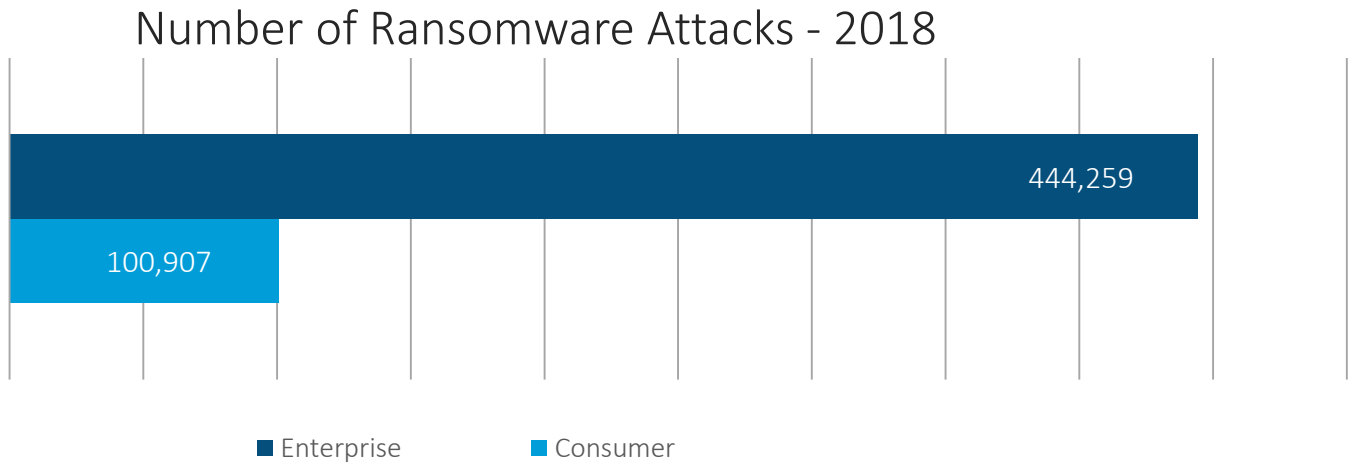
Ransomware Against Enterprises

Although there was a decrease in overall number of ransomware infections, enterprises saw a 12% increase in attacks.

* Internet Security Threat Report Volume 24 by Symantec

Ransomware





What can you do:

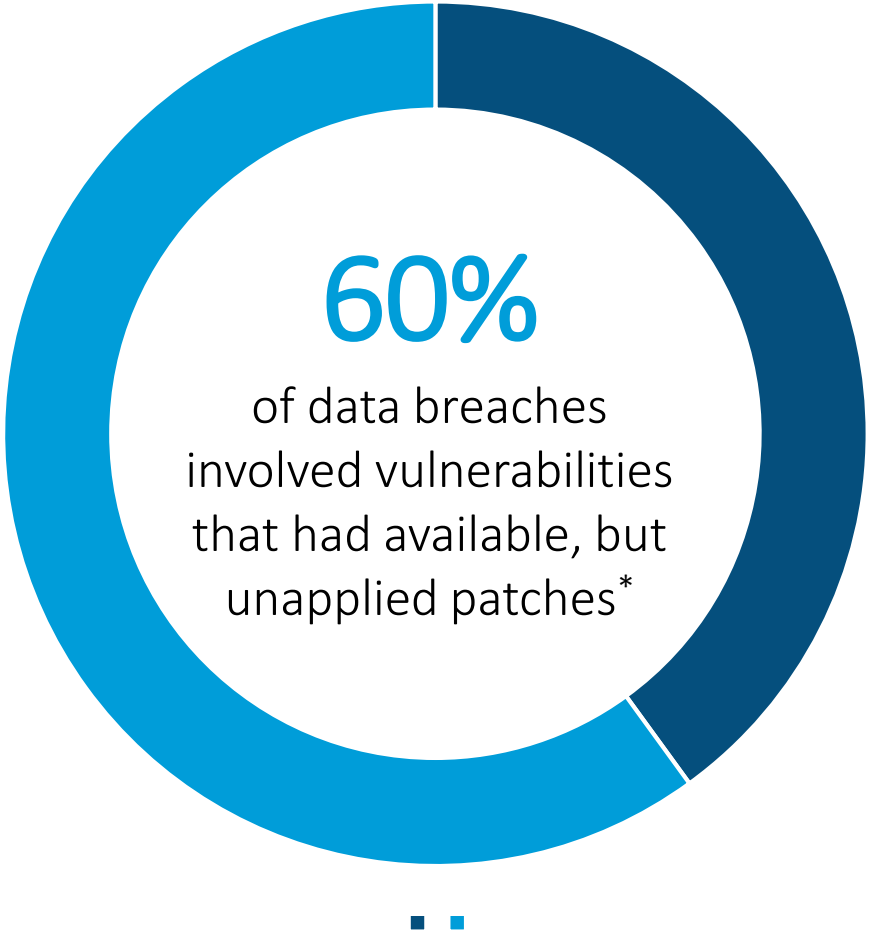
- Be wary of phishing emails
- Do not navigate to URLs you aren't absolutely sure are safe, through links or otherwise
- Never open attachments you weren't expecting
- Be wary of documents prompting you to enable Macros upon opening

* Internet Security Threat Report Volume 24 by Symantec

POLL

Does your organization have a formal security awareness training program that conducts regular phishing attempts?

Unpatched Systems and Out-of-Date Software



What can you do:

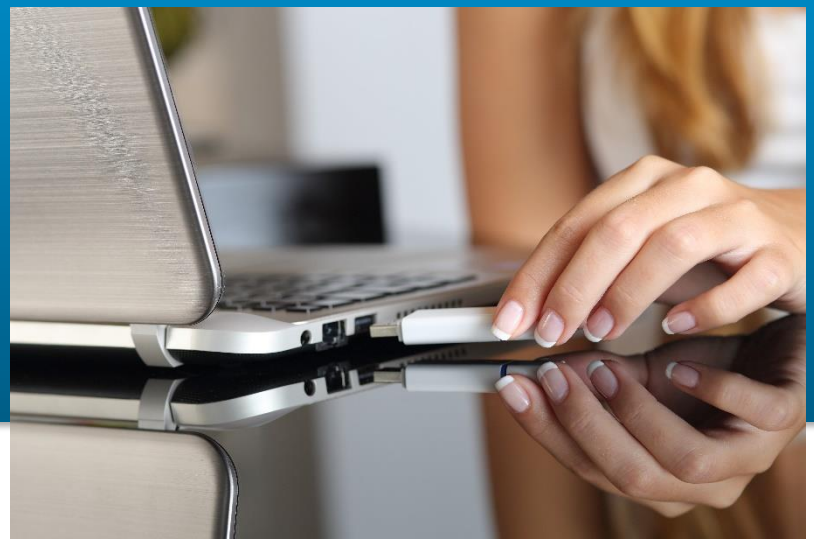
- Whether on your personal or work computer, make sure Microsoft and other applications are patched and up-to-date
- Ensure you are running antivirus software with the latest definitions

* https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Transferring Data to Unencrypted Devices

46% of Employees

admit to transferring data between their work and personal devices while working remotely*



What can you do:

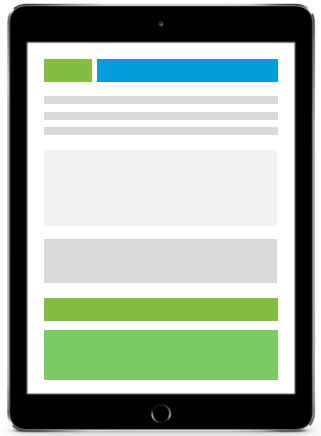
- Use company devices when working remotely, if possible
- Do not use work computers for personal use
- Do not save sensitive data to your personal device
- Do not save data to storage media unless it is encrypted
- Lock your device at home while not in use

* CISCO

Acquiring Lost or Stolen Devices

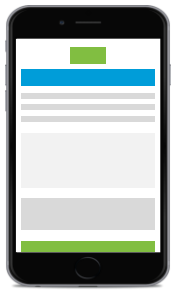
LAPTOP

An employee loses an unencrypted laptop



TABLET

A tablet is stolen from an employee's vehicle



PHONE

An employee's phone is forgotten at a coffee shop

What can you do:

- Utilize two-factor authentication (2FA)
- Logout or lock your device when it is not in use
- Do not save your logins and passwords on web forms or applications – rather use a password manager
- Do not share your credentials for devices, accounts, etc. with anyone

What can you do:

- Avoid using public Wi-Fi
- Check your phone and other device settings to ensure they do not auto-connect to public Wi-Fi
- Be wary of your surroundings when working in public spaces like coffee shops. Who can hear your conversation or look at your screen?

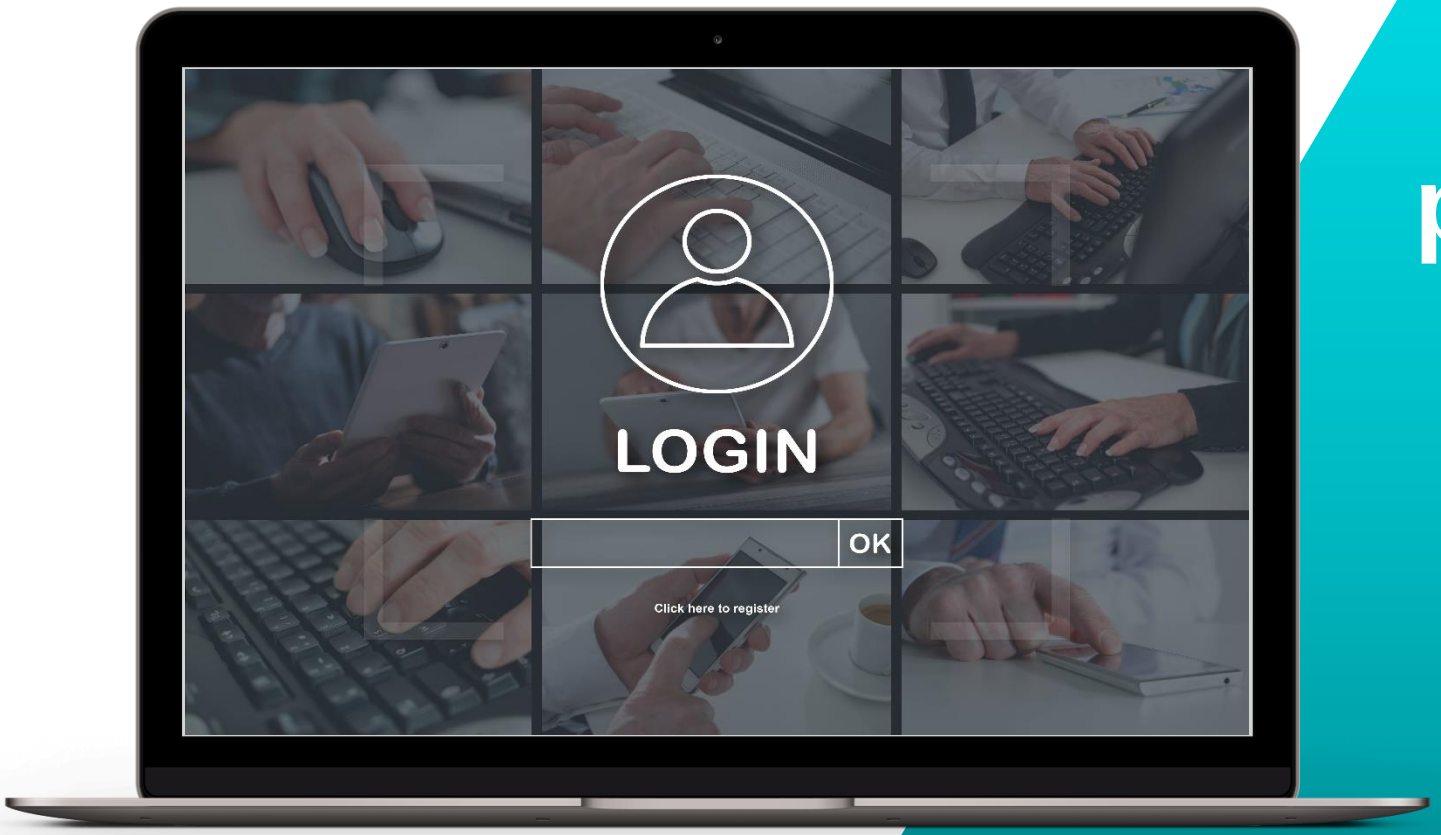
62%

of WiFi security incidents happen at cafes and coffee shops*

* https://amtrustfinancial.com/blog/small-business/remote-workers-and-cyber-liability

Supporting Remote Employees

Company Issued Devices



If possible, provide company issued devices for remote employees and make sure they are encrypted using full-disk encryption

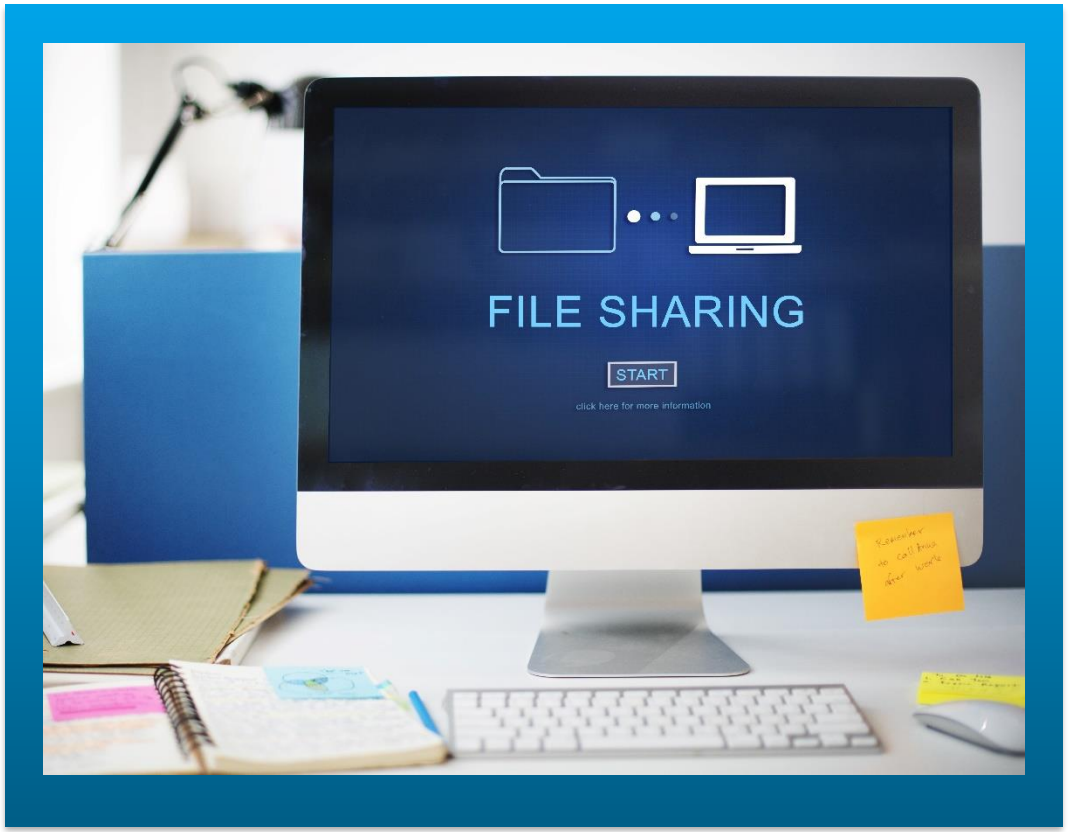
POLL

Does your organization provide devices to remote employees?

Setup VPN or Remote Desktop Protocols

Using a Virtual Private Network (VPN) or Remote Desktops allow employees to access company information through a secure, encrypted channel

Provide Secure File Sharing



- Setup email encryption to allow secure sharing of files and information
- Setup email alerts for incoming emails that may be phishing / spam
- Establish a secure file sharing system to allow for employees to collaborate while working from home

* https://openvpn.net/remote-workforce-cybersecurity-quick-poll/

Communicate IT Support's Availability

- Whether an in-house IT department or outside MSP, communicate IT support coverage hours with remote employees
- Hours could vary due to employee staffing models, alternating shifts, etc.
- Provide a set method to verify support staff's identity to reduce risk of impersonation using vishing (voice phishing)

* https://openvpn.net/remote-workforce-cybersecurity-quick-poll/

Provide Additional Training

- Provide training / offer a refresher course on important topics and functions:
  - Can you identify the top 5 characteristics of a phishing email?
  - How do you verify your MSP / IT Support staff?
  - What constitutes an incident and who do you contact?

Establish a Written Remote Work Policy

- Establish a written policy for remote workers
- Communicate the policy company-wide
- Provide additional training as necessary to ensure the policy is understood

Common Elements:

1. Require VPNs
2. Require sensitive data be encrypted
3. Prohibit work-related data on personal devices
4. Require ongoing training
5. Require use of a password manager*

* https://openvpn.net/remote-workforce-cybersecurity-quick-poll/

POLL

Does your organization have a remote work policy / procedure in place?

Questions?

Eric Vanderburg
Vice President, Cybersecurity
TCDI
216.664.1100 x226
e_vanderburg@tcdi.com

Bogdan Salamakha
Senior Cybersecuirty Engineer
TCDI
216.664.1100 x246
b_salamakha@tcdi.com

Frank Yako
CIO – Director of Strategic Initiatives
ASMGi
440.781.7515
fyako@asmgi.com