REMOTE WORK SECURITY

PREVENTING AND DETECTING CYBER INTRUSIONS IN A REMOTE WORK ENVIRONMENT

Presented by:

Chris Moschella, CPA, CISA

Senior Manager, Risk Advisory Services

Keiter

Your Opportunity Advisors

Experience | Knowledge | Relationships | Insight

Agenda

- Increase in Remote Work
- Impact to Security
- Securing Remote Workers

My prediction: A major surge in corporate data breaches stemming from weaknesses in remote work is on the way.

INCREASE IN REMOTE WORK

Increase in remote work

Microsoft Teams

March 19 – 44m daily users
April 29 – 75m daily users

Zoom

2019 – 10m daily participants
2020 – 300m daily participants

Citrix

Q1 FY20 - Subscriptions up 55% from Q1 FY19
Q1 YOY Revenue up 20%

Port 3389 – Remote Desktop

March 6 – 3 million
March 24 – 4.2 million
May 4 – 4.6 million

Remote work is here to stay

- Immediate future
  - Likely slow and phased return to physical offices
  - Google and Facebook work from home until end of year
- Long term
  - Likely significant increases in work from home (WFH) days
    - Nationwide Insurance moving all employees to hybrid WFH model and cutting leases at four major locations
    - Twitter email from Jack Dorsey (CEO) to staff – most employees can work from home forever
    - Google pulling out of deals for 2 million sq. ft. of office space
  - According to a recent survey from Gartner:
    - 75% of CFOs shifting at least 5% of jobs to permanent WFH
    - 6% of CFOs say half their workforce will make the switch
    - 57% of employees want to continue working from home and 48% feel more productive

Remote work is here to stay (con't)

- Long term
  - The Stanford Study
    - Saved monthly rent per employee
    - Attrition decreased by 50%
    - Shorter breaks
    - Fewer sick days
    - Took less vacation
    - However – More than half the group who worked remote 100% of the time felt too much isolation

Once we're past the COVID-induced work from home initiative, there will be a permanent effect on many knowledge workers.

IMPACT TO SECURITY

Impact to Security

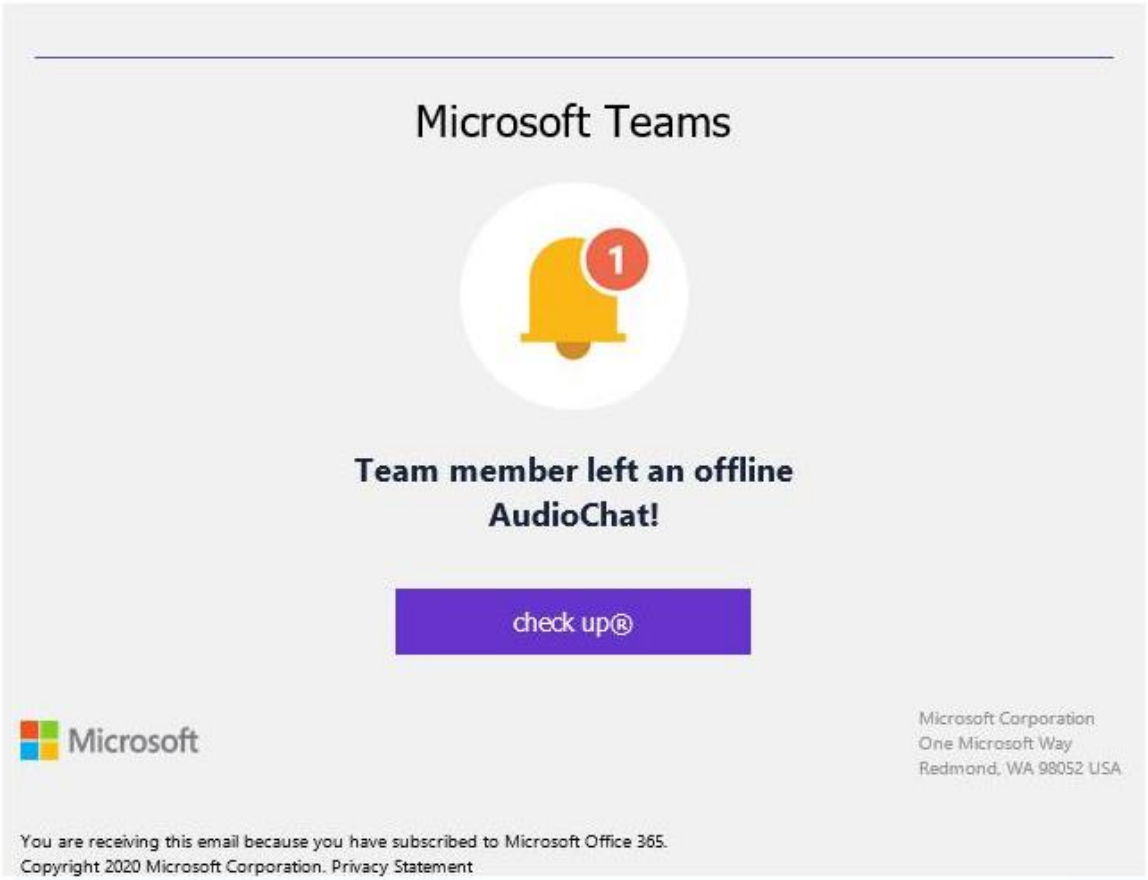
- Scams and Phishing
- Weaknesses in remote tooling
- Unsecured home networks

Scams and Phishing

- Scams take advantage of the COVID chaos
  - Phishing scams designed to confuse employees trying to work remotely and adjusting to using new tools
  - Phishing scams that capture sensitive data as part of stimulus checks
  - Selling fake vaccines and other drugs

Scams and Phishing

Subject: Chat Messaging in Teams®



- Actual example of a spear phish targeting a Keiter MS Teams user.

Weaknesses in Remote Tooling

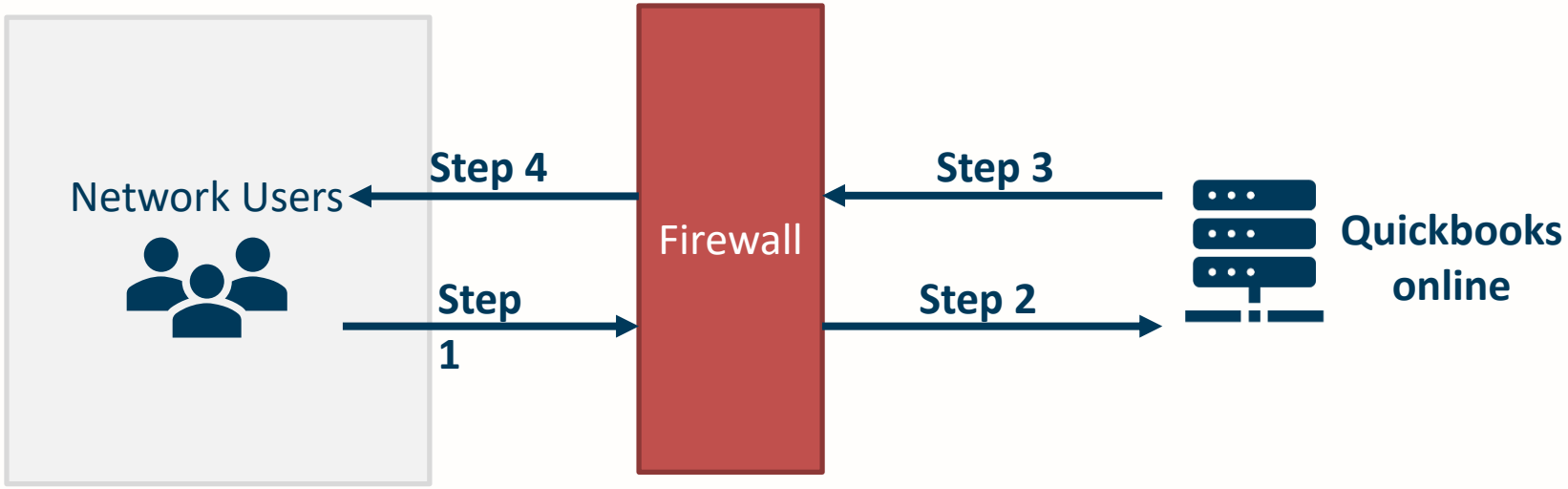
- The increase in use of remote access tools has drawn increased attention by threat actors.
- There have been well-publicized weaknesses in the tools businesses have rushed to embrace.
  - Zoom
  - Microsoft Teams
  - Cisco WebEx
- US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issues warning to businesses that have failed to implement best practices when deploying their Office 365 implementation.

Weaknesses in Home Networks

- Corporate networks generally protected by an enterprise-grade firewall
- Moving from a hardened corporate network to a home network creates new risks
  - Imagine giving every employee (and their families) the ability to control your corporate firewall.

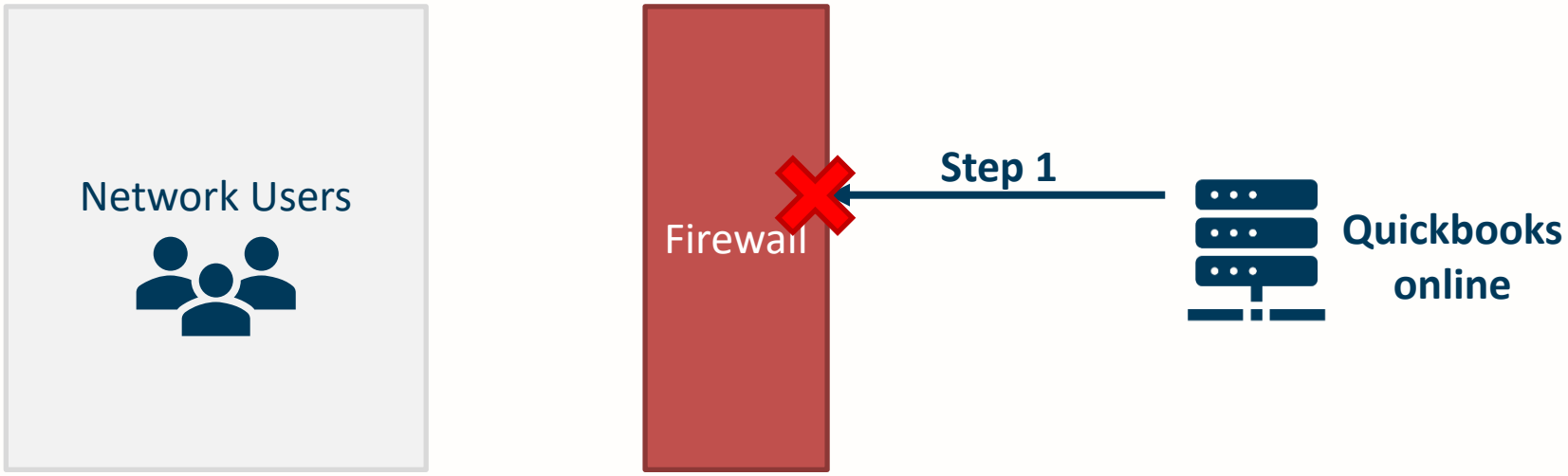
Firewalls

- Most firewalls are configured to allow outbound traffic, but to block most, if not all, incoming traffic.



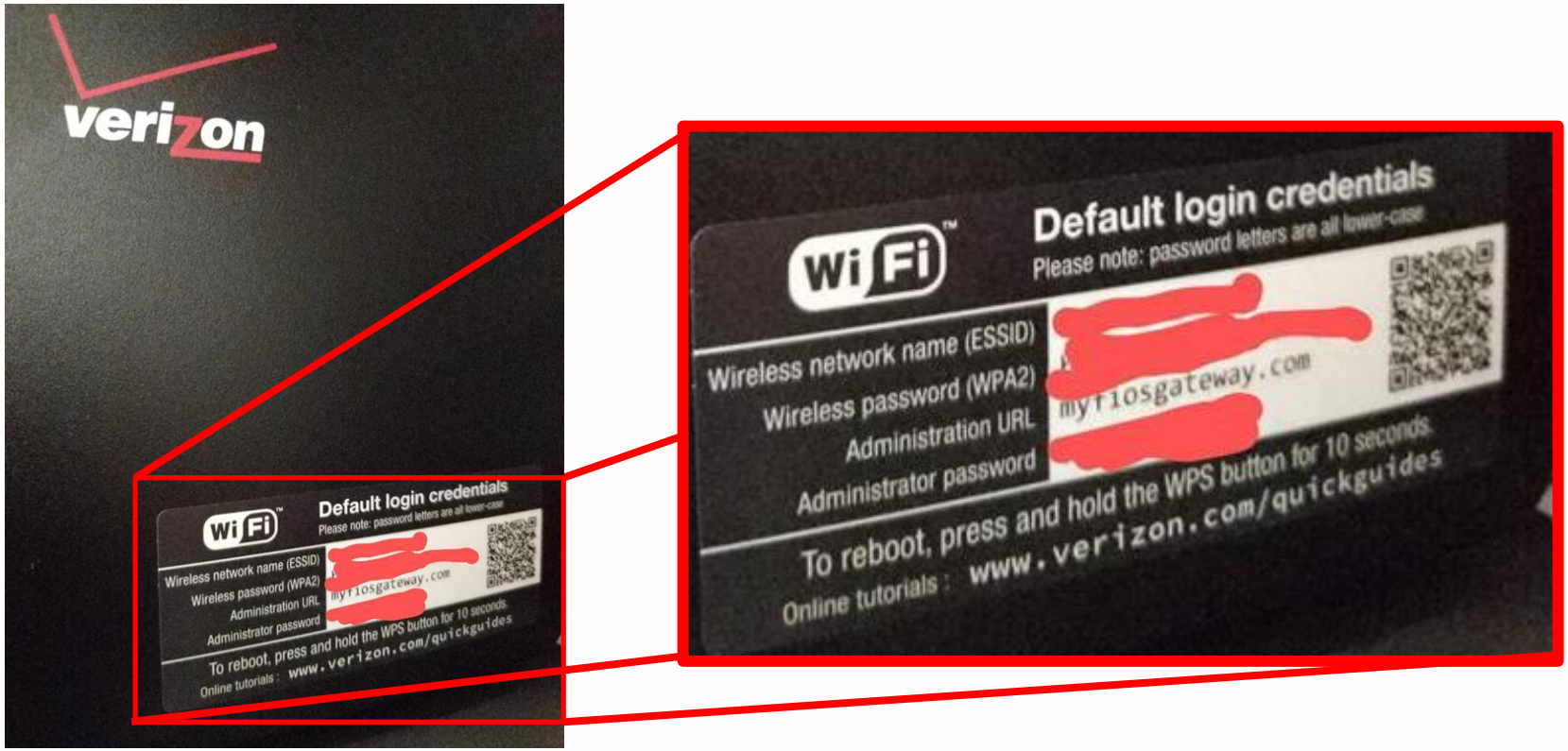
Firewalls

- Connections directly to the internal network are blocked



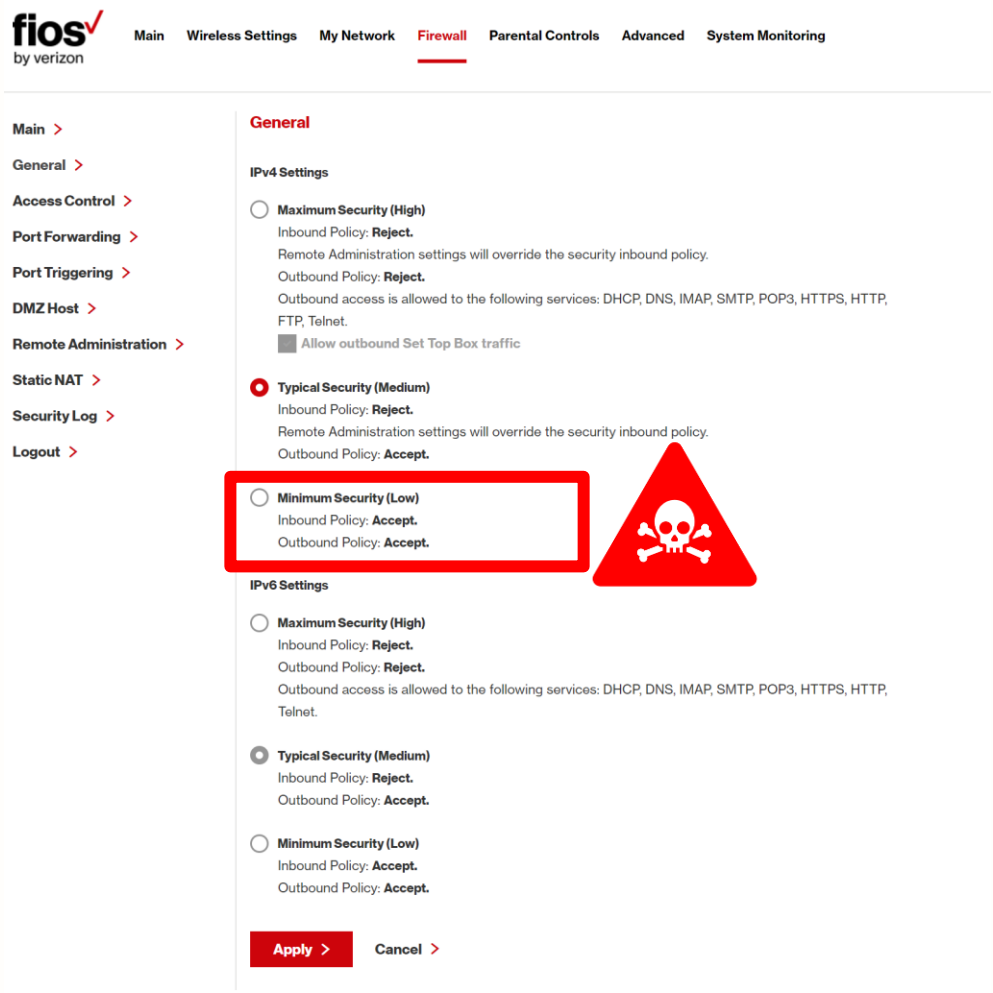
Home Networks – What can go wrong

- We have to assume that everyone who lives in your employee's home has access to the home router's administration functions.



Home Networks – What Can Go Wrong

Allowing Inbound Network Traffic



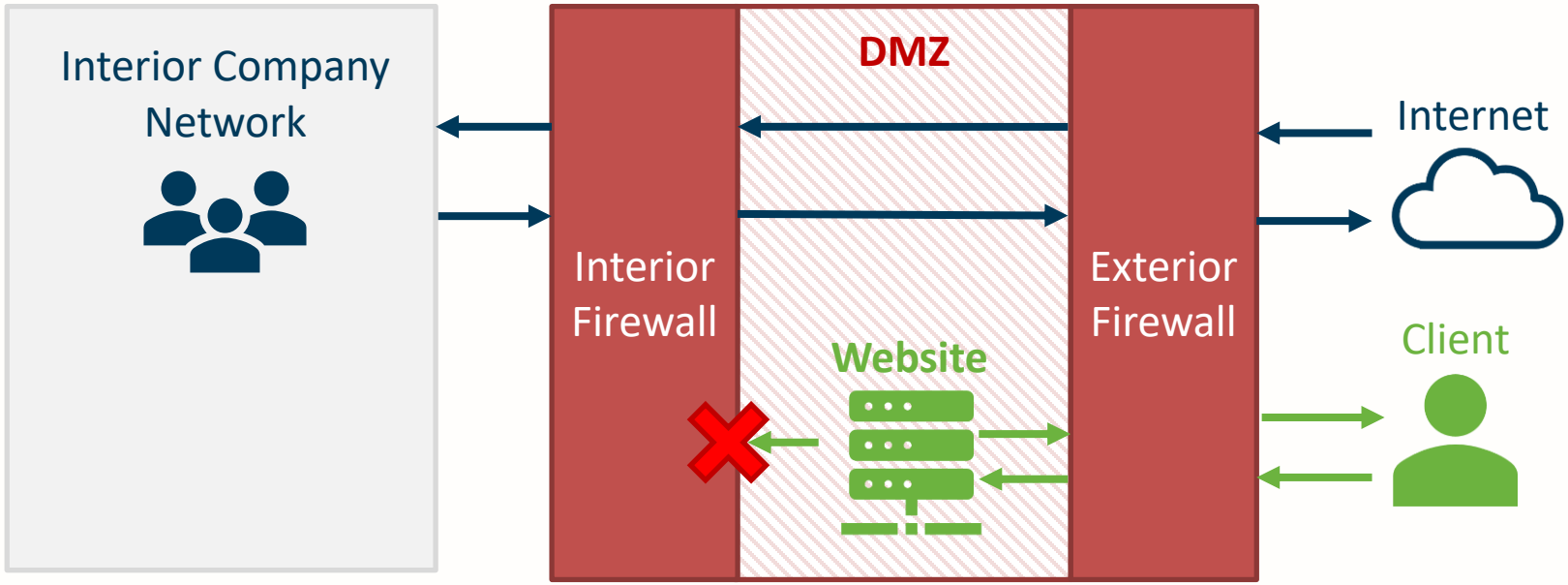
- With just a few clicks, your employee's home network can allow inbound connections.
- This is extremely dangerous and would never be allowed in a corporate network.

Home Networks – What Can Go Wrong

Improperly Configured DMZ

- A demilitarized zone (DMZ) on a network is a space where an organization can expose services (such as a website) to the public internet
- A properly configured DMZ allows a company to safely expose services without compromising the integrity of other resources on the internal network.

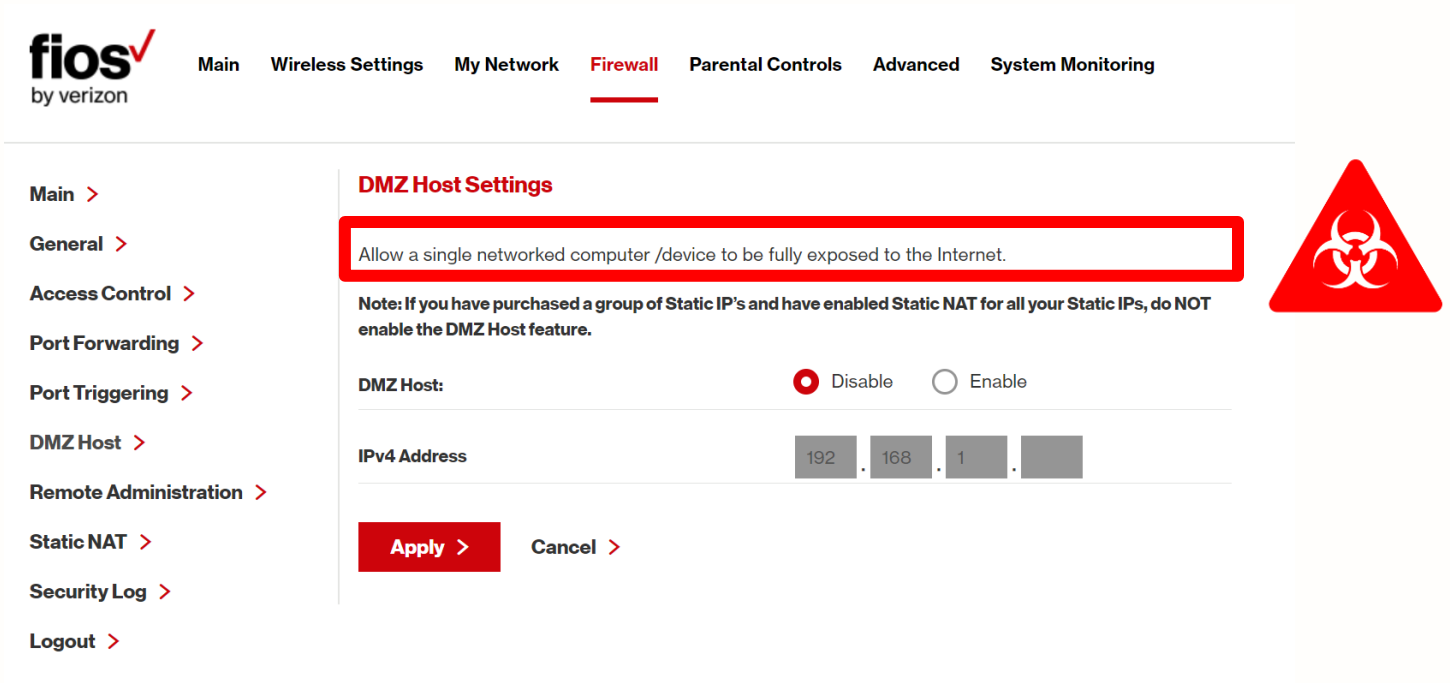
Example of a Properly Configured Corporate DMZ



Home Networks – What Can Go Wrong

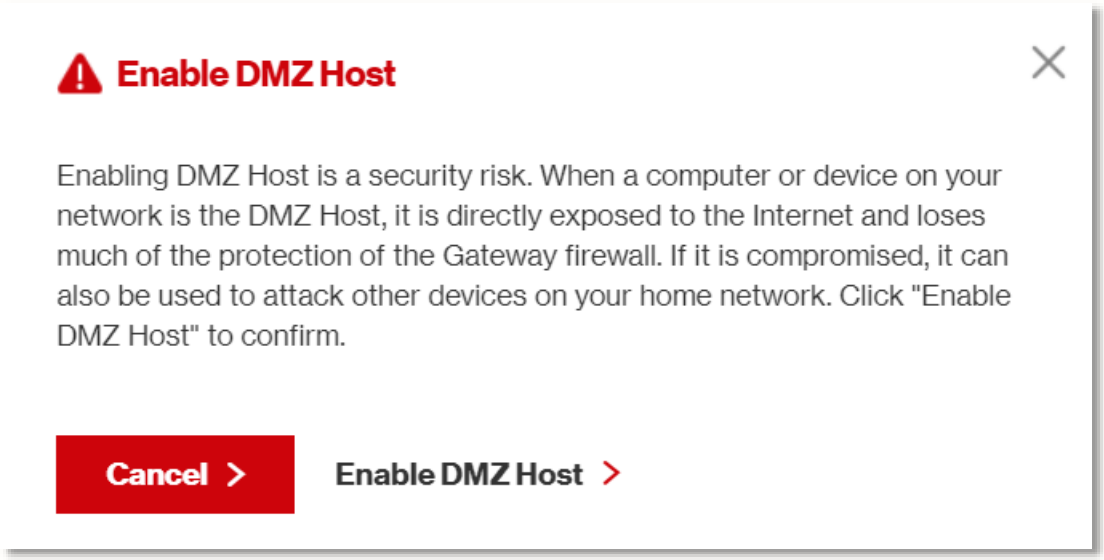
Improperly Configured DMZ

- Risk 1: Accidentally placing the company computer inside the DMZ
- Risk 2: Putting a device in the DMZ that is then compromised and used as a staging point for further intrusion



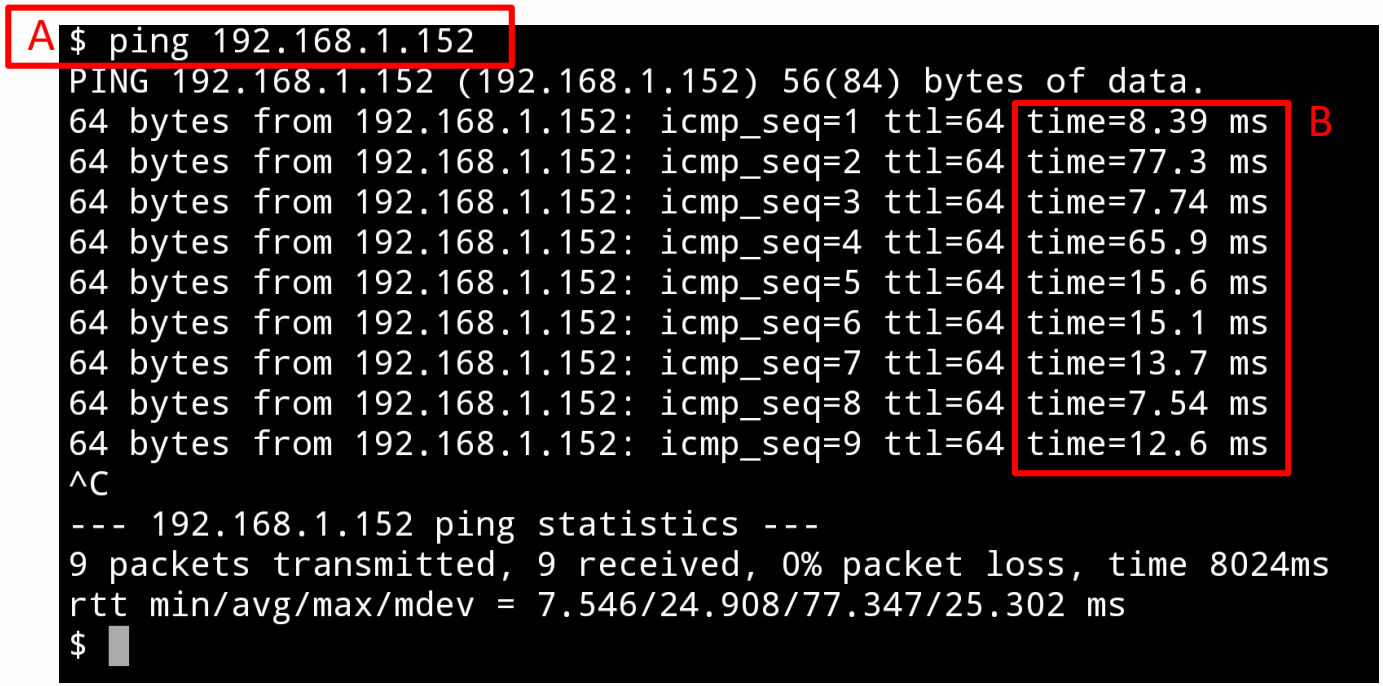
Home Networks – What Can Go Wrong

Improperly Configured DMZ



Home Networks – What Can Go Wrong

Improperly Configured DMZ



A ping command sent from the device in the DMZ to an IP address of a device outside the DMZ

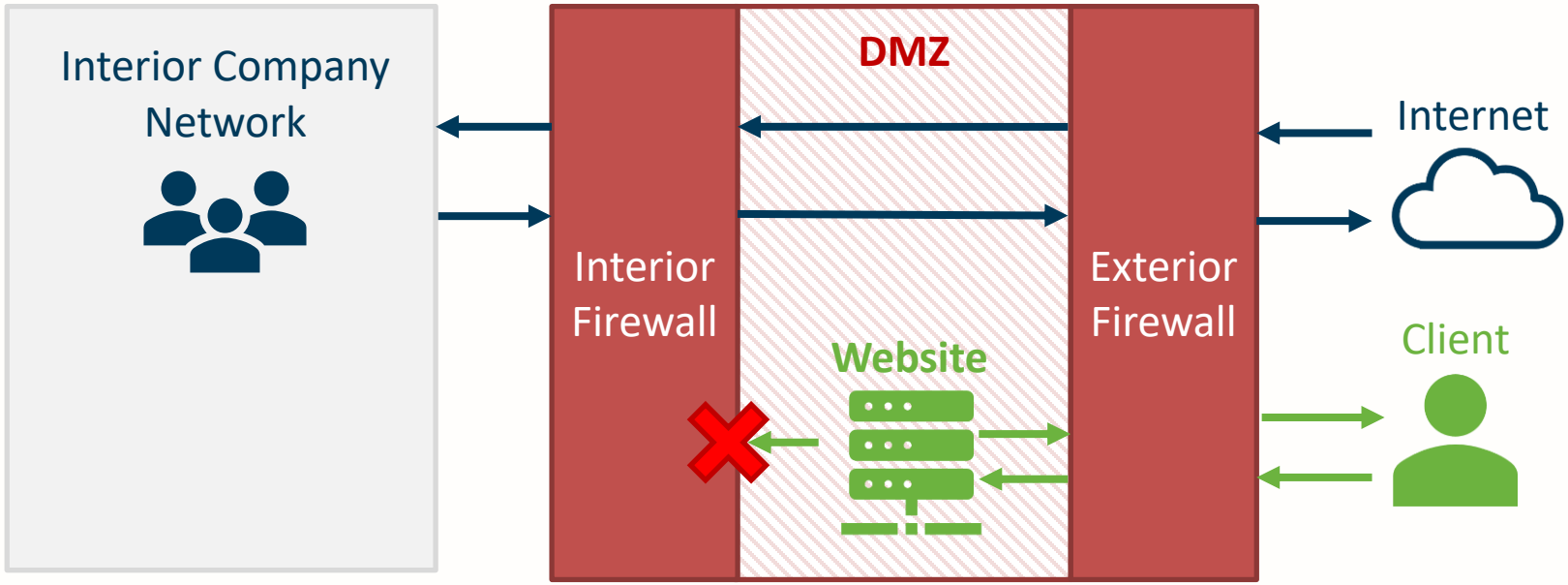
B Responses indicate the time it took the device to respond, confirming connectivity between the two

Home Networks – What Can Go Wrong

Improperly Configured DMZ

- In reality, a DMZ from a home router does not look like a good corporate DMZ

Example of a Properly Configured Corporate DMZ

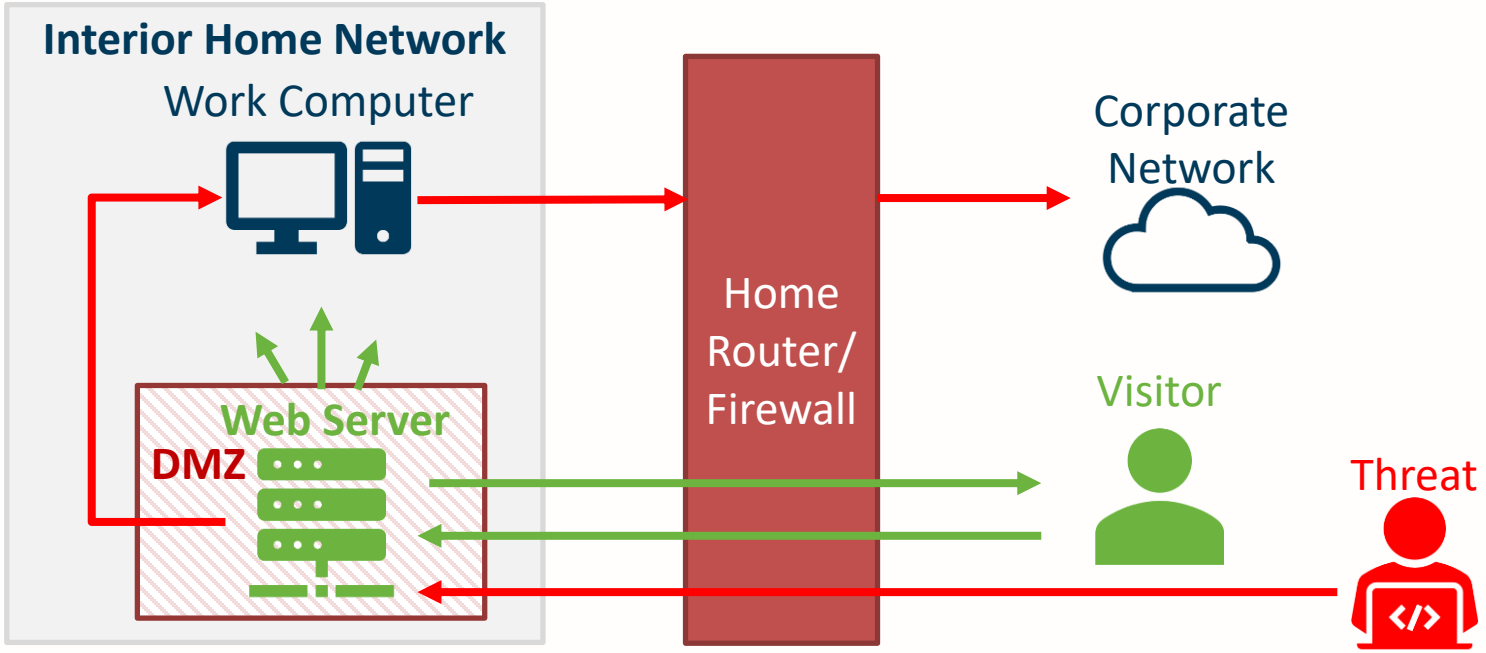


Home Networks – What Can Go Wrong

Improperly Configured DMZ

› In reality, a DMZ from a home router does not look like a real DMZ

Threat Path with DMZ on Home Router



Home Networks – What Can Go Wrong

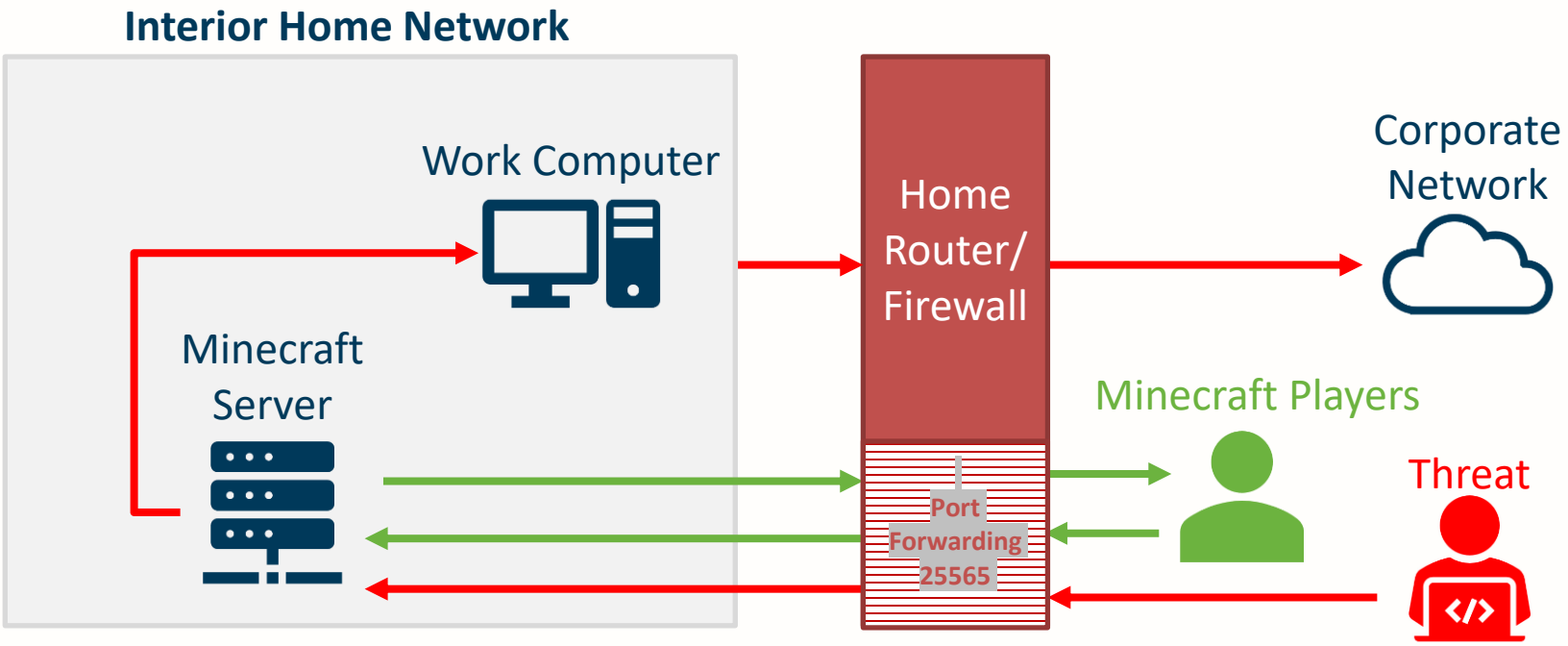
Port Forwarding

- What is a port?
  - A logical access (as opposed to physical) path through a network specified by a number
  - Over 65,000 ports. Examples:
    - https is port 443 – try google.com:443
    - http is port 80
    - ftp is port 21
    - SMTP (outbound email) is port 25
    - POP3 (inbound email) is port 110
    - Minecraft is port 25565

Home Networks – What Can Go Wrong

Port Forwarding

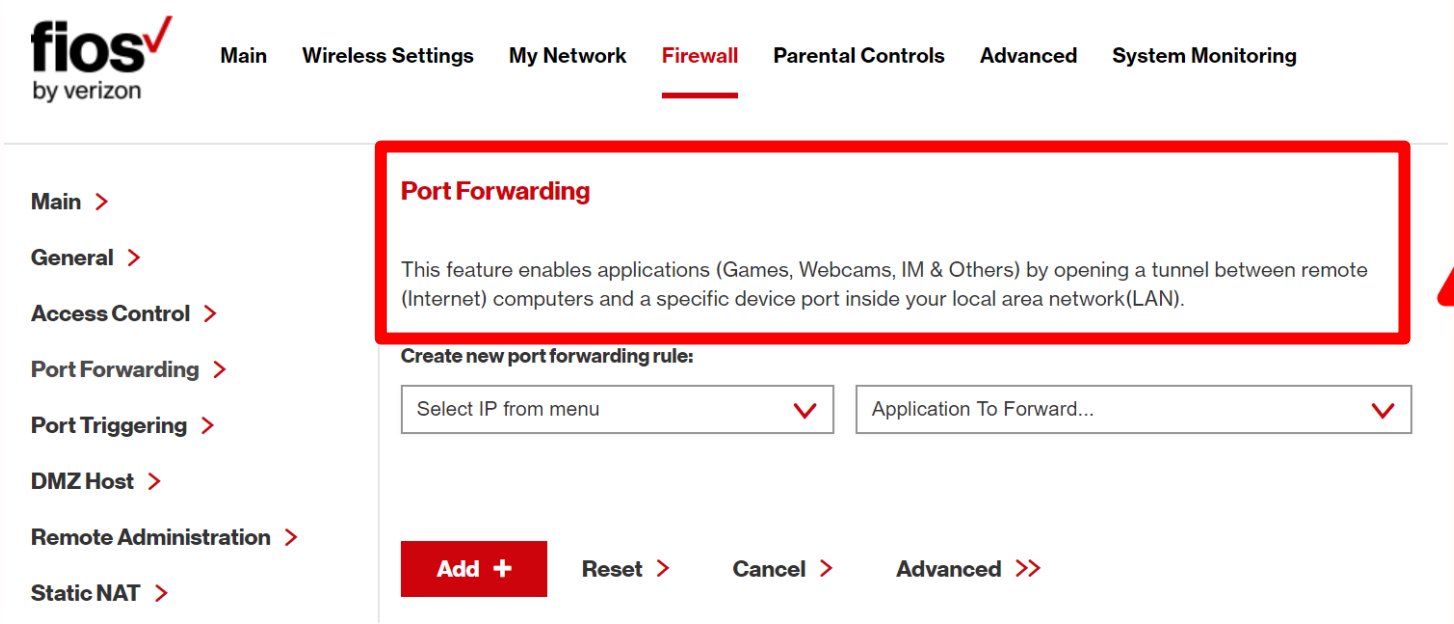
- A network device configured for port forwarding could be compromised and used as a staging point for further intrusion



Home Networks – What Can Go Wrong

Port Forwarding

- Corporate networks use properly configured DMZs to expose servers to the internet
- Port forwarding should not be used like this in a corporate environment



Home Networks – What Can Go Wrong

Other Risks

- Remote Home Router Administration
- Not using a Wi-Fi password or using a weak password
- Using Wi-Fi Protected Setup (WPS)
- Using Wired Equivalent Protocol (WEP)
- Existing malware or intrusions on other machines on the network (Windows 7)
- Having insecure internet of things on the network
- Having out of date router/firmware

SECURING REMOTE WORKERS

Securing Remote Workers

- Host-based firewalls
  - A “host” is simply any device connected to a network. A host-based firewall is a firewall installed on the device itself.
  - Restrictively configured host-based firewalls should block inbound connections to work computers from other devices on the network (with the exception of whitelisted corporate servers)
  - This will put significant barriers between threat actors on your home network and your work computer/work network.
  - Windows has a built-in firewall – but the default settings allow inbound connections.
    - Needs configuration to be properly secured

Securing Remote Workers

- Verify the security of your remote access configurations
  - RDP
  - Citrix
  - VPN

Securing Remote Workers

- Hard drive encryption
  - Many new laptops have been issued in the last two months.
  - Most users will store some amount of sensitive data on their computer, and for most businesses it is not a matter of ‘if’ but a matter of ‘when’ a laptop will be lost or stolen.
  - Depending on the jurisdiction, a lost laptop could meet the legal definition of a data breach and result in embarrassing and costly reporting to customers and authorities.
  - Encrypting the hard drive makes the hard drive unreadable to anyone who finds or steals a company computer.

Securing Remote Workers

- Multi-Factor Authentication for Remote Access
  - If users can remotely access your Virtual Private Network (VPN), Remote Desktop Service (RDS), Office 365, or other remote access tool, threat actors can as well.
  - MFA significantly reduces the risk from password phishing, weak passwords, or stolen passwords.

Securing Remote Workers

- Other Security Functions Continue to be Important
  - Anti-virus/Software Patching
  - Security Awareness Training & Phishing
    - Turn off computers at night
    - Reminder that company laptop is not a toy
    - Shredding printed protected info, e.g., PII, PHI, PCI
  - Web Filters
  - BYOD – Using home computers
  - Mobile Device Protection
  - Inactivity Screen Locks
  - Intrusion Detection – https://www.dragnet.io

Keiter Support

- Security Awareness Training
- Remote Access Focused Risk Assessments / Penetration Tests
- Technical review of:
  - VPN / Citrix / RDS Configuration Analysis
  - DMZ Configurations
  - Host-based firewall configurations
- Intrusion Detection – https://www.dragnet.io
  - Contact Chris Moschella – cmoschella@keitercpa.com for a demo.

Thank You!

Chris Moschella

cmoschella@keitercpa.com

(804) 419-2902