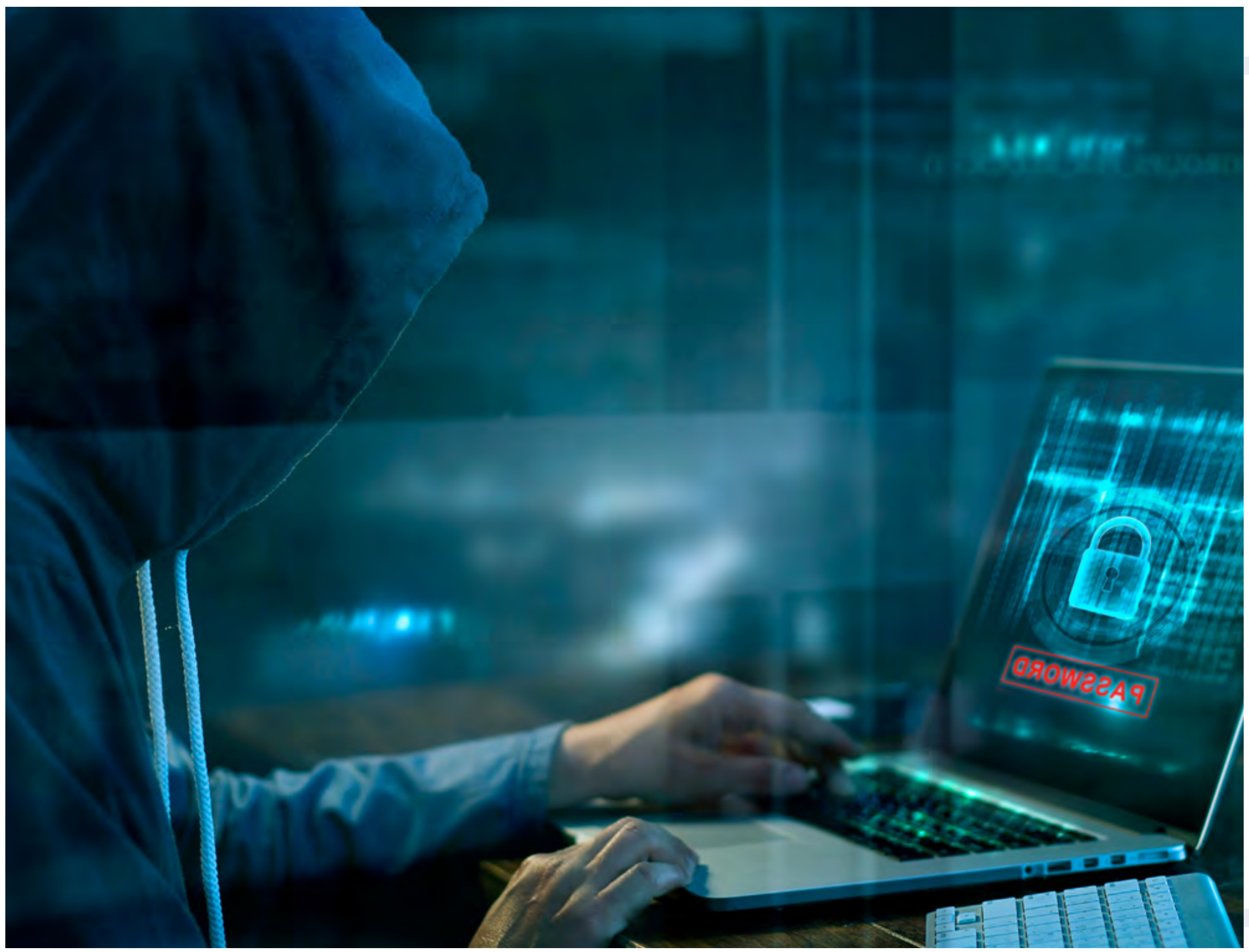
7 Tips to Improve Cyber Security While Working Remotely

A Digitech Systems, LLC eBook

Executive Summary



More people are working from home than ever before. In response, cyber criminals are shifting their focus to remote work setups, home networks and personal devices such as smartphones and tablets. There's no better time to revisit your strategies, products and services to make remote working secure.

In this ebook, you'll find information on how to eliminate the cyber security risks associated with working remotely. You'll read about the large number of data breaches that impact companies, including small businesses. You'll learn how Enterprise Content Management (ECM) systems are at the forefront of protecting organizations and their employees.

You will learn:

- Why each employee is vital to an organization's overall cyber security.
- How to secure a home office.
- The value of Virtual Private Networks (VPNs) for privacy and annonymity.
- Tips to create strong passwords and multi-factor authentification.
- The advantages of Enterprise Content Management systems.

Insights

Security is no longer a luxury.

A cyber emergency is the loss or compromise of company information or systems, typically through third-party intrusion, employee sabotage (cyber attacks), or an accident. A data breach is the release of confidential and other private information.

Of organizations that shifted to remote work as a result of the COVID-19 pandemic, 70% anticipate an increase in the cost of a data breach and 76% anticipate an increase in the time needed to identify and contain a potential breach, according to a 2020 study by IBM and Ponemon. The shift to remote work increased the average cost of a data breach by $137,000 to $4 million, the study reported. Only 21% of businesses utilize fully deployed security automation, the study found.

1. Threats don't come only from outsiders.

34% of data breaches involved internal actors. - Verizon

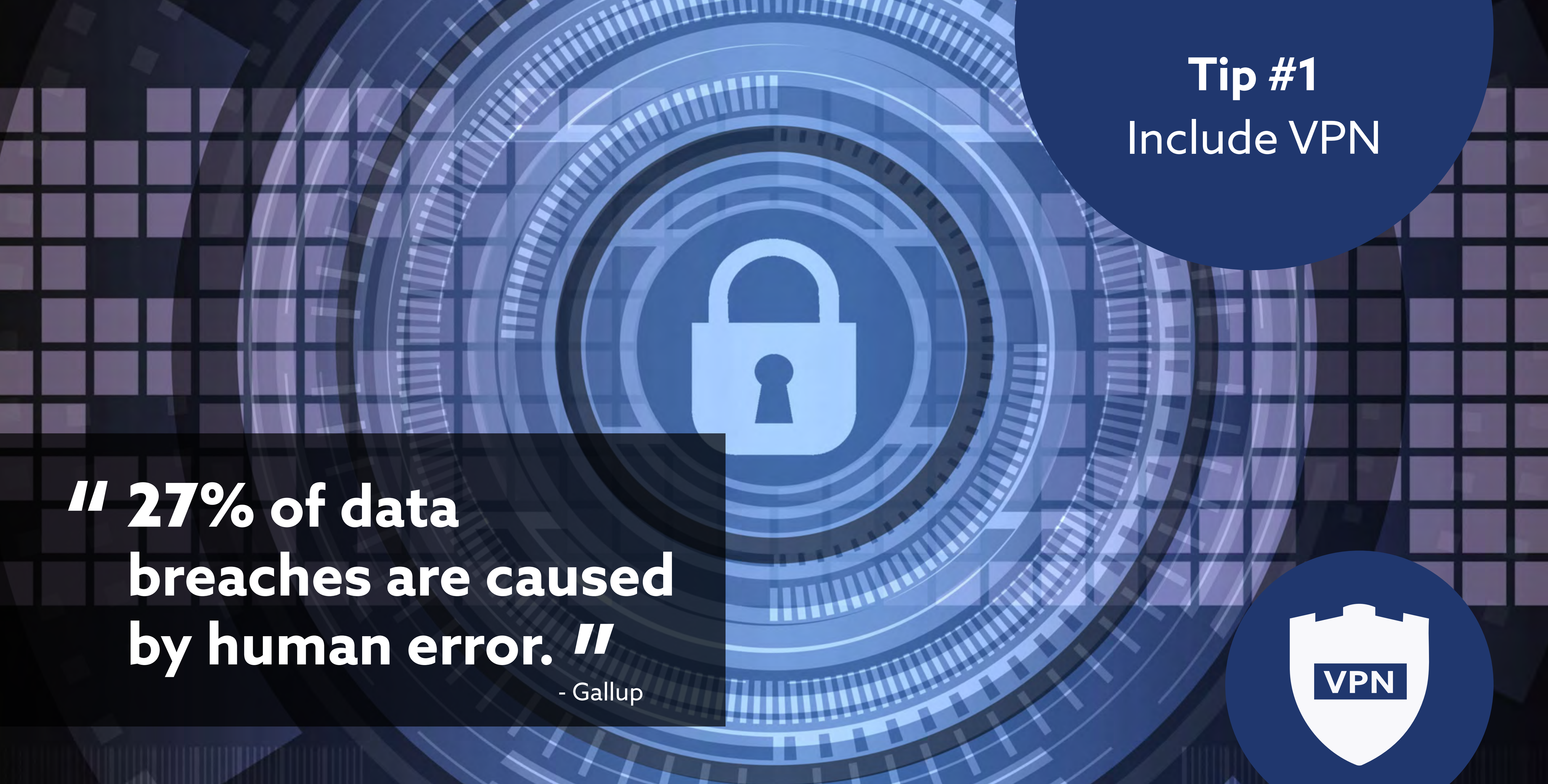
2. Most companies lack adequate protection.

79% of businesses do not use fully deployed security automation. -IBM/Ponemon.

3. Remote work brings added risks.

70% expect remote work to raise the costs of data breaches. - IBM/Ponemon

Use this guide and checklist to protect your data and privacy when working away from the office.



Tip #1
Include VPN

> **" 27% of data breaches are caused by human error. "**
>
> \- Gallup

Do you work with sensitive content? One of the best privacy protections is the use of a Virtual Private Network (VPN). A VPN makes it more difficult for cyber criminals and third parties to track your online activity and information.

VPNs work by masking a source's IP address so online actions are untraceable when a user is logging into a network from a remote location. VPNs offer privacy and anonymity. They enhance security of wireless connections.

Tip #2
Avoid Pop-Ups and Unknown Links

"92% of malware is delivered via email." - Verizon

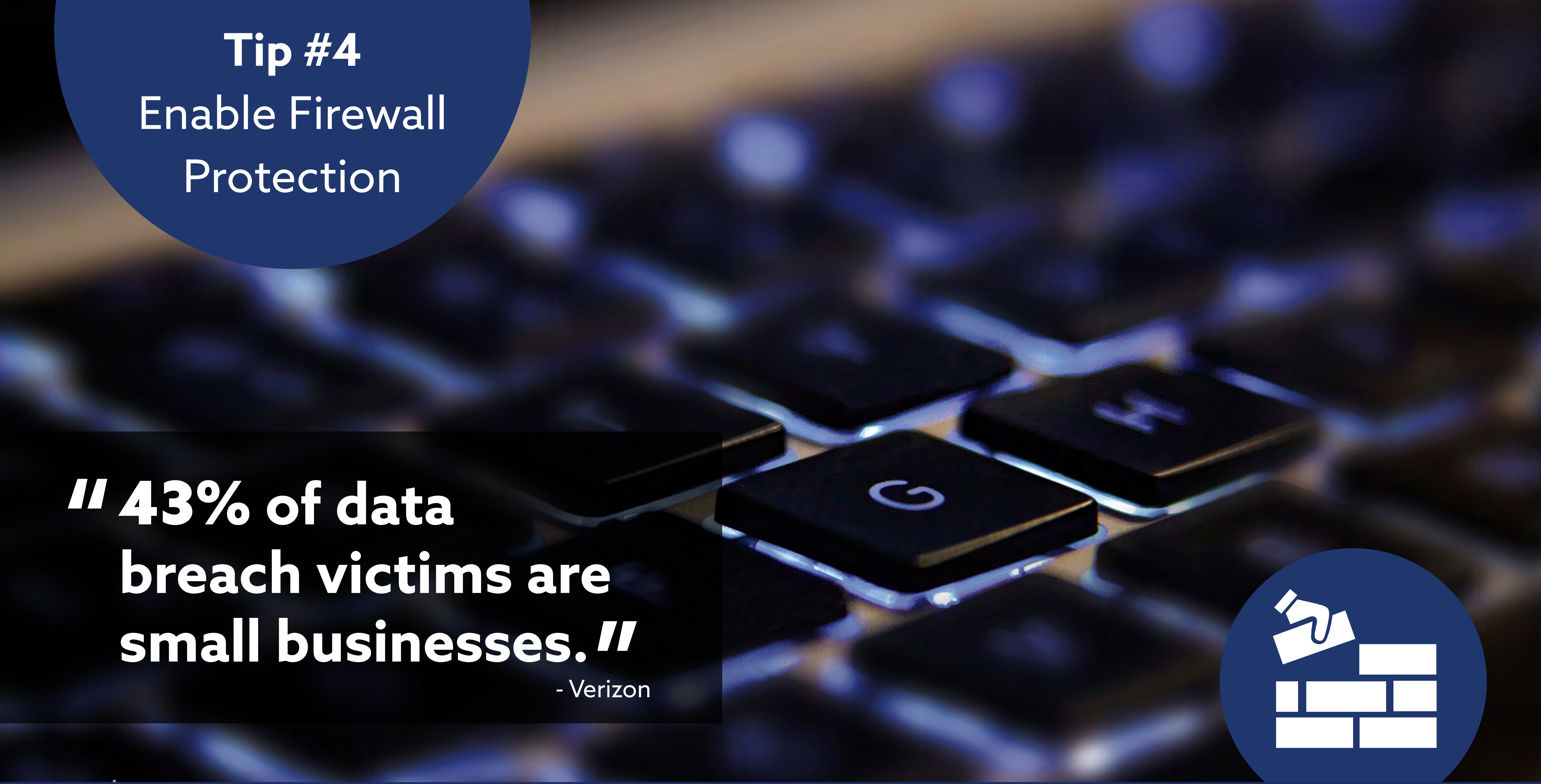
Pop-ups and unknown links are favorites of cyber criminals. They're the online version of a robocall but often more intrusive and damaging! Don't let scammers trick you into clicking on them and downloading malware. Steps you can take to protect yourself include: Install security software, be suspicious of requests for personal information, check the email sender's address and use unique passwords for files and apps.

Tip #3
Use Strong Password Protection and Authentication

> **"21% of files are not protected in any way."** - Varonis

Do you still think the best password protections are too complex? Think again. The use of strong passwords and authentication tools remains one of the top defenses against cyber snoops. And the tools are becoming more convenient as they are more sophisticated as part of a full Enterprise Content Management system.

Passwords should use a mix of at least 12 characters and get changed every 90 days. Authentication tools include security tokens and multi-factor identification. Widely available authenticator apps add to the choices for multi-factor protection beyond PINs, text messages, emails and telephone calls.



Tip #4
Enable Firewall Protection

"43% of data breach victims are small businesses."

- Verizon

Worried your employees are surfing online waters that should be off limits? Want to block outsiders from gaining access to your data? An Enterprise Content Management System helps you to set up and manage firewalls to control traffic on your computer network, including internet site access. Firewalls are basic protection but can be overlooked. In 2021 in Florida, a water utility was found to be without a firewall after an unsuccessful hack aimed at putting elevated chemicals into the water.

Tip #5
Regularly Install Security Updates

> **"It can cost almost $400,000 for every hour a server is down"**
>
> \- Statista

Because cyber criminals never stop, computer networks can go from secure to at risk in an instant. Regularly installed security updates protect against cyber attacks. Also, you should periodically review network logs to spot potential intruders or risk.

Hackers are innovative, Organizations should never rest because they think they've closed all of the security loopholes. Every company needs to stay informed on new threats and vulnerabilities in technology and work only with technologies that are diligent about developing solutions to meet any threat.

Tip #6
Use Secure Wi-Fi Connections

"71% of data breaches were financially motivated." - Verizon

You wouldn't discuss your most sensitive business transactions inside a crowded McDonald's, would you? An unsecure Wi-Fi network is kind of like that. It is susceptible to an outside cyber attack. Typically, home-based Wi-Fi setups are secure. For privacy, make sure you use a secure Wi-Fi connection. WPA2 is the current standard. As further protection, change your password regularly. Unsecure Wi-Fi is more commonly found in restaurants and other public places.

Tip #7
Don't Click .exe Files in Email

" 34% of data breaches involved internal actors. "

- Verizon

Don't open the front door to strangers; don't click on emails with unknown .exe files. A file with the EXE file extension is an executable file for opening software programs. Clicking on it is like opening the door to your computer. The person on the other side could be a cyber crook looking to access private information.

It's a reminder that you and your employees can play a big role in cyber security. Most data breaches are due in part to human error. Employee training is one of the most important – and, unfortunately, the most underfunded – activity in cybersecurity budgets, according to a report by Accenture.

Summary

Maintaining a good cyber security plan protects everyone, including remote workers. By following the 7 Steps to Improve Cyber Security While Working Remotely, employees who are away from the office can take take action on their own to protect themselves, their colleagues and their organization. Companywide, cyber security protections are a feature of the Enterprise Content Management products and services available from Digitech Systems. Digitech Systems products allow you to:

- Securely share and manage information from anywhere and on virtually any device.
- Improve efficiency through process automation.
- Manage more than 250 file types within a single application.
- Ensure document availability through 99.9% uptime guarantee.
- Enable hassle-free remote and telework strategies.
- and much more...

"54% agree that reliability is the most important factor in a cyber security solution"

- Zetta

Your Cyber Security Checklist

Save this helpful guide on the 7 Tips to Improve Cyber Security While Working Remotely.
Individual employees play a vital role in the overall protection of an organization.

1. Include VPN

Using a Virtual Private Network masks your IP address and protects you and your content from outside monitoring.

2. Avoid Pop-ups and Unknown Links

Other tips to stop malware: install security software, check email sender's address & guard personal information.

3. Strong Password Protection & Authentication

Use at least 12 characters for passwords. Authenticator apps go beyond PINs and text verifications.

4. Enable Firewall Protection

A firewall controls incoming and outgoing traffic on your computer network as well as internet site access.

5. Regularly Install Security Updates

Outdated security can open the door for cyber attacks. Also, review network logs to spot potential intruders or risks.

6. Use Secure Wi-Fi Connections

An unsecure connection like public-use Wi-fi leaves your content exposed. WPA2 is the current secure standard.

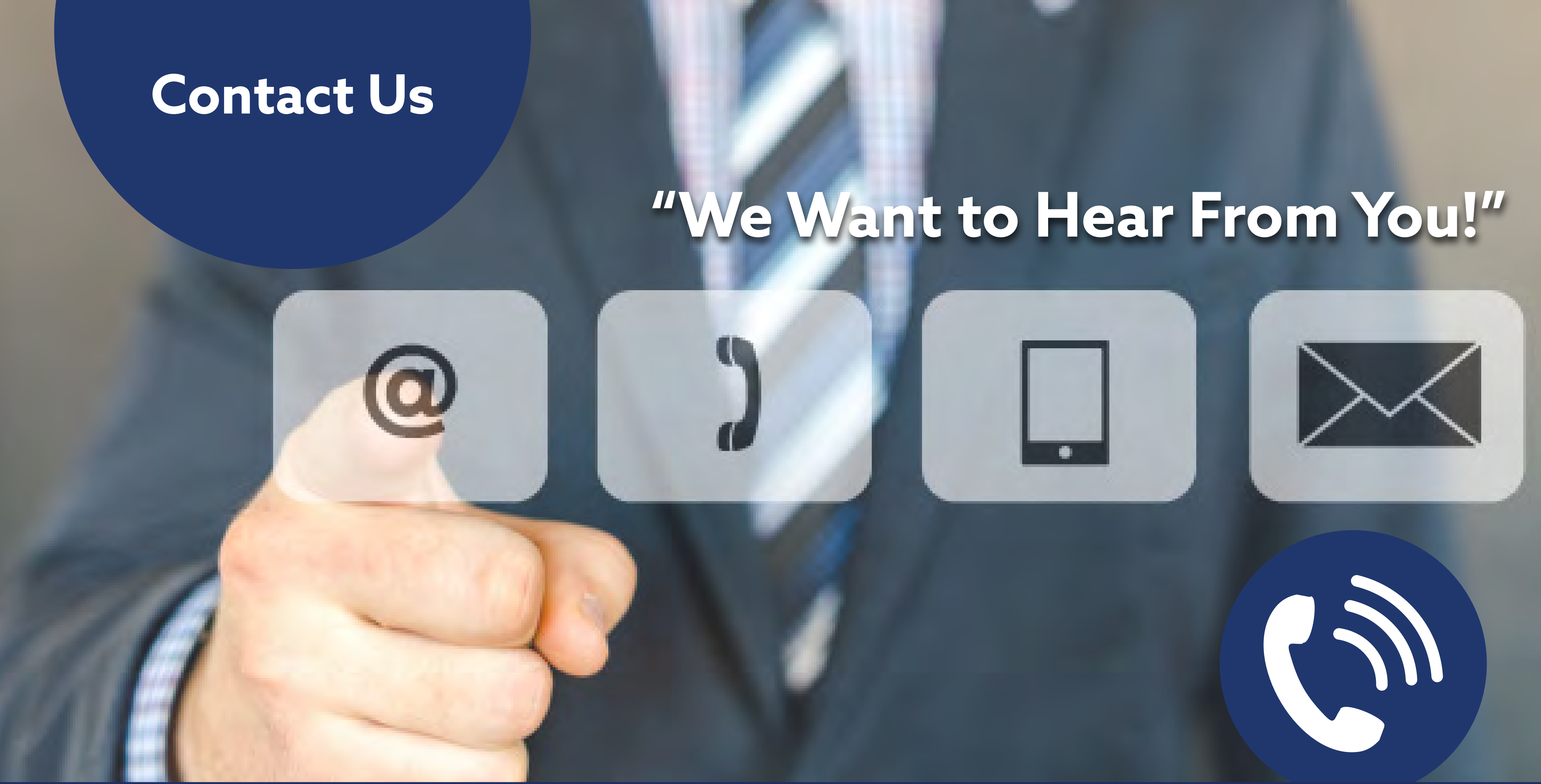
7. Don't Click .exe Files in Email

The EXE extension means it is an executable file that could unlock your computer to scammers.

Securing information systems and data against cyber emergencies is no longer a luxury. It is a necessity for all businesses. Each employee also plays an important role in helping their company maintain a secure environment whether in the office or working remotely. Studies show many data breaches occur due in part to human error.

Contact Us

"We Want to Hear From You!"



Corporate Headquarters
8400 E. Crescent Parkway, Suite 500
Greenwood Village, CO 80111
303.493.6900

TF: 866.374.3569
International: +1.303.493.6900

Lincoln, NE Office
8001 S. 15th St., Ste. A
Lincoln, NE 68512
402.484.7777

TF: 888.374.3569

LegendaryTechnicalSupport
Support Hours: 8 AM – 6 PM CST/CDT
TF: 877.374.3569
support@digitechsystems.com

Professional Services
TF: 855.374.3569
services@digitechps.com

DIGITECH SYSTEMS

Any Document • Anywhere • Anytime®

Contact us today to learn more about how you can improve your security while working remotely.

www.digitechsystems.com/features/cyber-security — 866.374.3569 — info@digitechsystems.com