In the last 15 years, the amount of work done remotely increased 173 percent. According to research and consulting firm Global Workplace Analytics, 3.6 percent of the total United States workforce works from home at least half-time under normal circumstances.

However, when situations arise at a regional or global level, employers may need employees to work remotely on a temporary basis.

As we see this shift from on-site to remote work, it’s important to reiterate security best practices and why they’re so important when working remotely.

Along with business travelers, remote workers are a frequent target of cybercriminals outside the workplace due to their remote access capabilities, vulnerability of off-site devices and networks and level of exposure.

The following topics, covered in more detail later, contribute to a secure remote environment for employees working outside the office:

- Secure connections
- Virtual meeting best practices
- Safe workspaces
- Phishing and social media awareness
- Approved devices and applications

While trends appear to indicate a continued increase in remote work, best practices can decrease risks within remote environments.

**STRATEGIES FOR STAYING SECURE**

- If your organization utilizes a virtual private network (VPN), use it to connect to organizational systems and resources.
- Never connect to an unsecured wireless network.
- Protect your home WiFi network with a unique, secure password. Do not use the default password on the router.
- Use only approved web video conferencing technology and be aware of what others can see.
- Keep your home or remote office organized and secure to protect data and devices.
- Beware of phishing and social media interactions targeted toward remote workers.
- Do not use personal applications/accounts or unapproved devices to complete work-related tasks.

**REMOTE WORK: A TRENDING TOPIC**

**SECURE CONNECTIONS**

- Virtual private networks (VPNs) and secure home networks.

**SAFE WORKSPACES**

- Securing remote physical workspaces and organizational data.

**PHISHING & SOCIAL MEDIA AWARENESS**

- Avoiding phishing and social media scams targeting remote workers.

**APPROVED DEVICES & APPLICATIONS**

- Using only approved devices and applications for work-related tasks.

**DISCREET WEB MEETINGS**

- Best practices for virtual meetings and conferences.

**ARM YOURSELF WITH SECURITY AWARENESS BEST PRACTICES RELEVANT TO WORK-FROM-HOME ENvironments.**
VIRTUAL PRIVATE NETWORK (VPN): THE SAFE CHOICE FOR A SECURE CONNECTION

A virtual private network (VPN) is a tool that can keep information safe as it travels across the internet. While your first step should always be to use a secure, password-protected WiFi connection, a VPN provides additional protection on both secure connections and public WiFi networks.

A VPN makes a direct, secure connection between your device and the private network of your organization. This connection is called a secure VPN tunnel. Data transferred through this tunnel is encrypted at both ends of the connection, so even if a cybercriminal is able to monitor data moving across the network, they will not be able to decrypt the data during transmission.

If your organization uses VPN technology for off-site connections to data, systems or networks, you should use the VPN connection every time you connect to an organization resource to protect any data that may be transferred.

As part of your preparation for working remotely, you should confirm your ability to connect securely to your organization’s network to protect data and communications while outside the office.

DON’T DEFAULT: SECURING A WIFI NETWORK

In-home WiFi networks can put organizations and their data at high risk if remote workers don’t take the proper steps to protect these networks before using them for work.

Your home WiFi network, whether established for personal use only or also for work purposes, should always be protected with a unique, secure password. Never use the default password provided with the router. This includes the password to join the network and the administrator password used to change router settings. Failure to do so may allow attackers to join the network nearby or remotely.

If you have guests in your home, it is also a good practice to create a separate guest WiFi network with an equally strong password that guests can use without the risk of compromising your regular network.

Additionally, if you are working outside the home, never connect to unsecured public wireless networks. Attackers often create fake networks in public spaces or monitor public connections to steal the data exchanged.
BE AWARE OF WHAT YOU SHARE: WEB & VIDEO CONFERENCING BEST PRACTICES

Recent industry metrics indicate that more than half of all meetings in enterprise-sized companies now utilize web conferencing technology.

With a rise in the use of these platforms, the unintentional sharing of information also increases.

The biggest risks related to web video conferencing technology involve background details and accidental exposure of information.

Your surroundings during a web meeting can reveal information present in the background that you don’t intend to broadcast. This might include calendars, schedules, project plans, notes or client information. Personal effects like family photos, educational degrees or valuables can also reveal details about you and your workspace that should not be shared.

In addition, many web conferencing platforms allow users to share their computer screen or documents with other participants. Accidentally displaying the wrong document may breach confidentiality, while an email pop-up or instant message notification may expose internal information clients shouldn’t see.

To prevent the potential for sharing incorrect or improper information, pre-load all documents and presentations for the meeting, keep open only the documents needed and close other programs and applications or temporarily disable notifications during the meeting.

These techniques can assist you not only in preventing accidental exposure of sensitive information but also projecting a professional, well-prepared image for you and your organization.

In addition to risks of unintentional exposure, platforms are also at risk of malicious exploits.

To protect against this risk, you should always install software updates as soon as they are available. You should also review the settings on your video conferencing software on a consistent basis to verify privacy and security protections are enabled.

Some vulnerabilities may involve attackers who activate webcams without the user’s knowledge. To mitigate this, disconnect external webcams when they are not in use. If your webcam is built into the device, use a webcam cover (even a basic solution like a sticky note or dark tape will work). If your webcam is compromised, an attacker’s view will be obstructed by a covered or disconnected camera.

VIDEO CONFERENCING TIPS

BLANK SPACE

Sit with your back to a blank wall or space. This prevents participants from seeing confidential information, electronics or other valuable items.

REDUCE CLUTTER

Remove unnecessary clutter from your space. Having a clean desk prevents accidental disclosure of information and projects a more positive image.

OBfuscation

Some video conferencing technologies allow you to hide your background. If this feature is available, use it to mask the area behind you.
REMOTE WORKSPACES: IDENTIFY THE RISKS

Working from a home office requires certain security considerations to protect your organization’s information, devices and systems. While there may be no malicious intent on the part of other members of your household, it’s still important to protect your workspace the same way you would in an on-site environment.

Keeping your home office as secure as an on-site workspace doesn’t have to be cumbersome. Note the items in the image below for tips to raise the security of your home workspace.

SECURE SHARING
You may be tempted to use a cloud service not approved by your organization outside the office. Err on the side of caution, not convenience.

LIMITED ACCESS
It’s best to locate your home office in a secure, lockable area of your home designated only for work and an area only you will use.

SAFE CONNECTION
Ensure that the connection you use at home is secure. Use a secure WiFi password, not the default password pre-loaded on your router.

SAFE STORAGE
Any work-related paper files should be stored in a locked file cabinet. Protecting physical data is just as important as protecting digital files.

LOCK DEVICES
Business devices used in the home should be locked and secured when you step away, just like in the workplace.

WORK USE ONLY
Use work devices only for work-related tasks. In addition, avoid allowing other family members to use devices designated for business use.

PERSONAL DEVICES
Ensure personal devices connected to your home network are safe and secure. Keep operating systems and anti-virus software up-to-date.
PHISHING: DON’T GET HOOKED AT HOME

Phishing attacks don’t stop when you’re working from home. In fact, remote workers are a potential focus of cybercriminals hoping to catch employees off guard and take advantage of a change in operational circumstances.

Remote workers should be particularly cautious in reviewing emails that claim to come from internal IT teams, those that request credentials or confidential information, emails that inquire about your position or role in the organization and any messages that offer to update software via a download.

Additionally, once a cybercriminal knows that a target is a remote worker, they may attempt to exploit devices and networks you’re using in your home office or conduct more advanced social engineering. Avoid disclosing the fact that you are working from home.

Phishing links remain the most common means of delivering malware. Never click links or open attachments in a suspicious email. Instead, report the email following your organization’s policies and delete the message. If you do click a link or open an attachment from a suspicious email, immediately notify your IT helpdesk.

Cybercriminals may target you via phone calls (vishing) and text messages (SMiShing), so use caution with these communication methods as well and do not divulge information.

TIPS TO AVOID PHISHING ATTACKS

- Review all emails carefully for elements that indicate a phishing attack.
- Generic greetings, poor grammar and urgent warnings are red flags.
- Avoid opening emails with suspicious or suggestive subject lines.
- Never click on links or open attachments in a suspicious email.
- Use caution with odd or unfamiliar senders or unusual emails from known senders.
- Never respond to a suspicious email. Instead, report it immediately.
- Notify your IT helpdesk immediately if you clicked on a suspicious link or attachment.
- Be cautious with emails that have odd “to” and/or “from” addresses.
- Carefully monitor phone calls and text messages for signs of vishing or SMiShing.

EMAIL SECURITY BEST PRACTICES
PROTECT YOUR HOME WORKSPACE ENVIRONMENT AND YOUR ORGANIZATION’S SYSTEMS AND DATA.
SAFE SHARING: LIMITING INFORMATION EXPOSURE ON SOCIAL MEDIA NETWORKS

Millions of users are now connected on multiple social media platforms. A segment of this network population includes cybercriminals, lurking for information about you and your organization to use in attacks.

Remote workers who overshare details about their work situation, technology, positions and projects risk bringing unwanted attention from attackers by providing easily-accessible information.

Limit the amount of information you share on social media, both work-related and personal, to avoid overexposure. Remote workers, in particular, should avoid disclosing their work-from-home status.

SUSPICIOUS ADS
While many ads on social media sites are legitimate marketing, avoid any that mention “shocking videos,” offer free gift cards and or link to unfamiliar websites.

HIDDEN LINKS
Social media posts and links often include links to other sites. Treat all links with suspicion and click carefully.

CURRENT LOCATION
Never post your location or mention when you’re away from home. This can be an open invitation to a burglar searching for a vulnerability.

SOCIAL MEDIA POLICIES
Before posting information about your employer on social media or connecting to social media sites on work devices, ensure you understand and follow your corporate social media policy adequately.

UNUSUAL MESSAGES
If you receive a message from a known contact, be certain the tone matches the supposed sender. Watch out for spoofed accounts sending phishing messages.

SENSITIVE INFORMATION
Don’t post private details. This includes information about you and your employer. Use caution with photos as well.

FAKE EMAILS
Don’t click links in emails that appear to come from social media sites. This is a common phishing scam to entice users to give up their credentials.

REMOTE WORKER STATUS
If you work remotely, do not disclose this information via social media. Doing so allows a cybercriminal to quickly identify you as a potential target for attacks focused on remote workers.

YOU SHOULD KNOW

SOCIAL MEDIA: BEST PRACTICES

While many ads on social media sites are legitimate marketing, avoid any that mention “shocking videos,” offer free gift cards and or link to unfamiliar websites.

Social media posts and links often include links to other sites. Treat all links with suspicion and click carefully.

Never post your location or mention when you’re away from home. This can be an open invitation to a burglar searching for a vulnerability.

Before posting information about your employer on social media or connecting to social media sites on work devices, ensure you understand and follow your corporate social media policy adequately.

If you receive a message from a known contact, be certain the tone matches the supposed sender. Watch out for spoofed accounts sending phishing messages.

Don’t post private details. This includes information about you and your employer. Use caution with photos as well.

Don’t click links in emails that appear to come from social media sites. This is a common phishing scam to entice users to give up their credentials.

If you work remotely, do not disclose this information via social media. Doing so allows a cybercriminal to quickly identify you as a potential target for attacks focused on remote workers.
NOTHING PERSONAL: APPROVED APPLICATIONS

Using applications or services that are not explicitly approved by your organization to complete work tasks or store and share work-related data introduces tremendous risk.

It may be tempting to employ a service or application you utilize in your personal life to make your job easier. However, you may not be considering the dangers involved with using a tool that may not meet your organization’s standards.

Used improperly, an unapproved application or service could lead to data loss, theft of intellectual property, compliance violations, malware, contractual breaches or data exposure.

You have a responsibility, even more so as a remote worker, to use only the applications and services approved by your organization.

Organizations perform detailed reviews of the technologies used to process, store and share information to ensure their compliance and security before implementation. Circumventing policies by using unapproved applications or services violates the trust your organization places in you to protect its data.

Similarly, using your employer’s applications or services for personal tasks or storage not only violates policies, but can expose the organization’s data to compromise if malware is introduced into the environment through your personal use.

Do not mix personal and work data, applications or services to protect yourself and the organization.

SOUND ADVICE: USE AN APPROVED DEVICE

Because organizations have no control over unapproved devices, they should never be connected to an organization’s network or resources.

Always follow your organization’s policies regarding device and system usage outside the office.

Whether your organization provides a device or allows you to use a personal device for work, you should ensure that the operating system and applications are kept up to date, enable a secure lock/unlock method, encrypt devices that can access sensitive data and only take the device during travel when it is necessary.

To protect the device from potential malicious connections, you should disable autoconnect for both WiFi and Bluetooth in the device’s settings and disconnect any existing connections when they are not in use.

In case of theft, you should also make an inventory list of all electronics used for work, including the manufacturer, model and serial number, and you should enable the “Find My Phone” or remote wipe software on devices.

Portable devices like phones or tablets should be locked in a file cabinet or safe when not in use. All devices should have a password-protected lock screen enabled and you should lock the device any time you step away.

All data stored on devices used for work should be backed up regularly to a location approved by your organization.

It is imperative that remote workers only utilize devices approved by their organization to reduce the risk of data or network compromise.