8 SECURITY THREATS FOR REMOTE WORKSTATIONS

And How You Can Mitigate Your Risk

EAST ATLANTIC SECURITY

28 Schenck Parkway, Suite 200
Asheville, NC 28803

888.354.6208
rex.nance@EastAtlanticSecurity.com

8 Security Threats for Remote Workstations

And How You Can Mitigate Your Risk

In 2020, the Covid-19 pandemic created unique challenges for companies with regards to work-from-home conditions and network security. With many employees continuing to work remotely, cybercriminals are taking full advantage of unsecured home workstations to gain access to company networks.

It's no surprise that we're seeing increased scams and phishing attempts targeting telecommuters, whose home networks are typically not as secure as corporate offices. Experts are expecting this to accelerate. Some of the factors:

- Remote workstations pose specific risks and require additional security measures, staff training, and work-from-home protocols in order to keep the corporate network secure.

- Due to the urgency of the situation, most companies didn't have time and resources to set up secure workstations, company devices, and protocols for remote employees.
- For a variety of reasons, employees working remotely are more vulnerable to falling prey to phishing emails and other scams, potentially giving cybercriminals direct access to the corporate network.

Authorities warn that these and other factors create the perfect storm for cybercriminals.

What do employers need to do to secure their employees' remote workstations and protect company data?

In order to fully secure your company network, you need the services of a qualified IT security technician to perform more advanced security measures. ***However, that may not be feasible for you at this time.*** The measures below will help reduce the risks inherent with remote workstations.

1. Company Device

When possible, a company-issued laptop is the safest workstation: It's a known entity and uses the company's application suite and anti-virus. Be aware, however, that as soon as that device leaves the office and goes remote it becomes a security threat, depending on where and how an employee accesses company data.

Ideally, an employee will have a company-supplied, dedicated laptop that's *only used for work*. However, given the work situation in response to the Covid-19 pandemic, employers might have no other option than to allow employees to use a personal computer for work. We'll address that later.

A foundational caveat for using a company laptop: DO NOT USE FOR ANY PERSONAL USE. This includes signing into personal email accounts, social

networks, NOTHING; do not even sign in for a quick check. *Doing so can unwittingly open the door for hackers to gain access to the company's network.*

2. Public Wi-Fi

All public Wi-Fi should be considered unsafe, and untrusted. Accessing data even on a password-protected public Wi-Fi connection at say, Starbucks, is different than from home. You might think that getting the password from the barista and signing directly into their Wi-Fi connection is secure; ***however, anyone can fire up a hot spot*** and give it the same name and password as Starbucks' Wi-Fi. If an employee signs onto that one by mistake—an easy and common mistake to make--they've unknowingly given that person direct access to their device and potentially or indirectly, the company network.

Depending on what kind of provider Starbucks has, they may be able to restrict access between wireless nodes; do they do this? Who knows? Does the barista know? Probably not.

Best advice, while at a place like Starbucks, access via your own hot spot or VPN if you have one on your company laptop. *DO NOT access at Starbucks or any public Wi-Fi unless you have one of these options.*

3. Accessing Company Resources and VPNs

Another scenario is what kind of resources do employees need access to? Can they get everything they need to do their job with just an internet connection? **Users will probably need to access resources that are in their corporate offices.** They can do that with a VPN, which the employer needs to set up or have an IT technician do so.

The problem with a VPN is that if the employee needs to use a personal machine at home, the employer has no control over that machine. Once the employee has connected, they've opened a tunnel from their home network to your office network. *This gives cybercriminals direct access.*

The risk increases if the employee's network or device is already infected with spyware, malware, viruses, etc.

An employee's personal device needs to be considered an untrusted workstation.

Employers have the ability to implement a sophisticated VPN from an untrusted workstation back to the corporate network, allowing that user access to specific resources from restricted channels, so if there was someone spying on their workstation, they wouldn't have access to the full corporate network.

This doesn't make it an excellent solution, but it can reduce your security risk by up to around 80%.

4. Passwords and Two-Factor Authentication

Using time-saving features like autocomplete and saving passwords on your browser is tempting. What specific security risks do these habits pose?

Websites can put in hidden fields in a webpage and your browser will autofill them. Hackers can potentially get your email address, street address, phone number, and other personal information. ***And with that information, you can be compromised.***

- Turn off **autocomplete**, and any saved passwords.
- Better solution: Use a **password management app**, like LastPass.
- Follow current industry recommendations for **secure, unique passwords**. (LastPass will generate secure passwords for you!)

Enabling two-factor authentication is an easy way to tighten security and should be used for all accounts.

5. Firewalls

Use firewalls for personal networks. Always have your provider firewall enabled, like Windows. Depending on how many devices you have on your home network, you should go even deeper than an anti-virus like Webroot.

Don't rely on your ISP access point or anything it provides. Go out and buy your own security device or firewall and plug it into theirs--and then keep it updated. Some recommendations:

- Sonicwall Tz105 UTM
- Cisco RV110W
- Ubiquity UniFi USG

Get a hardware firewall hooked up that allows you to create virtual networks. Put your primary computer on one, and IOT devices on a separate network with no access to the computer in case an IOT device gets compromised.

Be aware, there are major security flaws for the top firewall manufacturers on the market. ***You must keep up with recent patches as soon as they're released***.

A common problem that an employer may now be facing is this: A patch was announced but it wasn't concerning at the time because they didn't VPN. It didn't seem relevant, so they opted not to install it. Now suddenly, they're sending employees home to work, they turn on their (unpatched) VPN, and now they're exposed.

Backstory on Patches
A lot of security flaws are found by ethical hackers, who then notify the manufacturers. The ethical hackers release the exploit the day the manufacturers have promised the patch release, which notifies the public of the security flaw. If the patches don't get applied immediately, the operating system will be vulnerable; unethical hackers can now exploit that flaw. **It's imperative to keep your operating systems current and updated.**

Forbes' article published in January of 2020 is an excellent read: "U.S. Government Issues Powerful Security Alert: Upgrade VPN Or Expect Cyber Attacks."

6. Phishing emails

Phishing emails are more difficult to detect when working from home. When an email seems to have come from a co-worker or superior, it's harder to verify it; you can't just call across the room and say, "Hey Joe, did you send this?" to verify its authenticity.

Protocols for Emails:

- Do not click on any links in an email, unless you can verify the source--especially on a mobile device, where the link is difficult to investigate. Hover your mouse over the link and look at the URL and verify its origin.
- *Don't open PDFs, Word docs, images, or any attachments that come in an email without first verifying with the sender.*
- Don't reply via email to verify the contents with the sender. The hacker that sent it to you can reply. **Call on the phone to verify.**
- **Don't send personal info through email.** Legitimate businesses will never request you to do so.

Safest practice: Flag any email from the internet, set the server to pre-pin a warning in the body of the email to state that "this originated from the internet." That way if someone sends you something and they're faking your CEO, you will know right away that it came from the internet.

In Exchange you can create a "transport rule" and it routes things for you. I have a client who likes to be copied on every email that comes into the company from outside the organization.

Make sure you have a corporate policy in place stating that employees have no rights to privacy when it to comes to email, and that they should not be using their work email for personal purposes.

7. Beware of Bogus Websites, Apps

Phishing emails and bogus websites centered around information about current events can crop up by the thousands (e.g. apps with global tracking maps during the pandemic containing spyware and malware.).

This has become a huge problem, as people are falling prey to this tactic. **Do not seek information from untrusted sources.** Doing so can compromise your device and the company network.

8. Personal Devices

Back to using personal devices for work. **An employee's personal device can be managed through a Bring Your Own Device policy;** if you don't have one in place, you really don't want people using their own devices.

Either use a VPN when connecting remotely, or Microsoft cloud offering.

Best Practice: Use Microsoft Windows Virtual Desktop in the cloud. You can build a full shared virtual desktop in the Azure cloud and establish a VPN connection between the Azure network and the company network via the cloud. If you have a compromised workstation, that compromise can't cross to the Microsoft host without sign-in credentials and multi-factor authentication.

Using your personal phone or tablet to check work emails, files, etc. is a big NO when working from home. If, however, employees are expected to respond to email during off-hours via phone, then Office 365 is the safest way to do so. With Mobile Device Management, you can set policies and settings that will help control access to your organization's email and documents. You can also remotely wipe a lost or stolen device to remove sensitive information. You can read more about this on Microsoft's Support page.

In the event an employee's device is infected with malware, spyware, etc., Mobile Device Management sets up a "business space" and will keep that area separated and protected from the rest of the items on the device.

Want Help Ensuring That Your Company Has All 10 Of These Covered?

If you're concerned about the dangers of cybercriminals gaining access to your network, call us for an audit of your current IT systems.

We will conduct a **CyberSecurity Risk Assessment** of your company's overall network health to review and validate data-loss and security loopholes. The audit analyzes your infrastructure, IT security, managed support and services, and communications. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, and home PCs.

This assessment is valued at $997 and is available at no charge in this offer only, for a limited time.

At the end of this assessment, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files—usually much longer than you anticipated.

- Are your employees freely using the Internet to access risky websites or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are put in place frequently and it's easy to violate one without being aware; however, you'd still suffer the bad PR and fines.

- Is your firewall and antivirus configured properly and updated?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate that nothing was overlooked.

You Are Under No Obligation to Do or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our CyberSecurity Risk Assessment. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for your needs remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to provide this service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 888-354-6208 or you can e-mail me personally at rex.nance@EastAtlanticSecurity.com.

Dedicated to serving you,

Rex Nance, CEO
East Atlantic Security, LLC

EAST ATLANTIC
SECURITY

www.EastAtlanticSecurity.com
rex.nance@EastAtlanticSecurity.com

What Our Clients are Saying:

"Choosing the right technology partner is one of the most strategic decisions you will make. Beyond the need for a trusted IT manager, sales opportunities require hands-on experience to close and navigate implementation. With Rex's team behind us, we've become competitive with mammoth corporations, and more importantly, we win sales opportunities from clients looking for customization, flexibility, and a personal touch from a technology perspective. From desktop troubleshooting to supporting our biggest ROIs, East Atlantic Security is there until the job is finished. We're investing in a seasoned business partner that tailors any and all tech services to our needs." (Pictured below running the Tough Mudder)

Aimee Schleizer
Chief Financial Officer
MeritCard Solutions

"East Atlantic Security consistently provides fabulous service in IT, including database design and management, custom software solutions, monitoring and maintaining networks, data backups and PCI compliance work. I trust East Atlantic Security to monitor our network 24/7 and get the job done quickly and effectively so we can move our business forward without having to hire expensive IT resources. Give them a call--you will be glad you did."

Tom Marsan
Vice President
SignaPay

"We had a server failure late in the day. East Atlantic Security was recommended to us and we couldn't be more pleased. They came out that evening and consulted with us throughout the weekend and into the following week, providing us with several options and prices. They got us back up and running in a timely manner. We experienced not only great service at a competitive price, but they also made themselves available to answer additional questions, even during non-business hours. I highly recommend them."

David Whatley
Managing Partner
AutoRealty, LLC

What to Do Now

If you'd like a free CyberSecurity Risk Assessment, do one of the following:

1. **Complete and fax the enclosed "Fast Action" response form.**
2. We will call you to schedule a convenient time for your assessment. There is no obligation for you to buy or do anything.

You can also call us at 888-354-6208, or schedule online at:
https://eastatlanticsecurity.com/8-security-threats-download/

Fast Action Response Form:

☐ "Yes! I would like to schedule a free CyberSecurity Risk Assessment so I can be certain my business network and data are protected. I understand that I'm under NO obligation to do or buy anything by signing up for this audit.

Please Complete and Fax Back:

Name: _____

Title: _____

Company: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone: _____ Fax: _____

E-mail: _____

Fax This Form To: 828-761-0060

Or Call: 888-354-6208

Or schedule online at:

https://eastatlanticsecurity.com/8-security-threats-download/