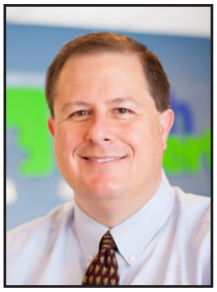
November 2023

TechTidbit.com

brought to you by Tech Experts

Five Habits Your Smart Remote Workers Should Have



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Remote work has become a way of life very quickly, hasn't it? Loads of businesses and their people are reaping the rewards of flexibility and convenience.

But it also brings cyber security challenges that demand your attention. Of course, this should always be a concern, but when you have employees working from home, a coffee shop, or anywhere else for that matter, you need to make sure they're making wise decisions that put the security of your data at the forefront.

These are five habits your remote workers should adopt straight away.

Choose your work location wisely

Working from a favorite coffee shop or a picturesque park may seem like a dream come true, but it can expose you to more cyber security risks. Over-the-shoulder attacks, where cyber criminals discreetly snoop on your screen in public spaces, might seem unlikely, but they have real potential to lead to data breaches.

Employees should choose to work in quieter, more private settings to minimize this risk.

Beware of public Wi-Fi

Public Wi-Fi networks are a common breeding ground for cyber threats. If your people must work from a public place, ask them to avoid connecting to public Wi-Fi. These networks can be less secure and make you vulnerable to hacking. Instead, use your phone's hotspot for a safer internet connection. And a VPN (Virtual Private Network) encrypts data.

Invest in security software

This serves as a protective shield against malware and cyber attacks. It's a valuable addition to both company-provided and personal devices. Not only does it safeguard business data, but it can also shield your personal information, such as credit card details and sensitive documents.

Keep everything updated

Regularly updating all your devices is not just about gaining access to new features; it's also about staying secure. Software updates contain crucial security fixes that patch vulnerabilities.

Remember, it's not just laptops and phones that need updating, but also routers and any IoT (Internet of Things) devices connected to your network.

Manage household risks

Even within the confines of their homes, computers hold sensitive business information. If your employees have housemates, children, or other family members sharing their space, ask them to consider implementing parental controls to prevent accidental data breaches.

By adopting these smart habits, as well as taking the right security measures, you can let your people enjoy the benefits of remote work – while everything stays secure and safe.

If we can help keep your remote setups secure, get in touch.

Even within the confines of their homes, computers hold sensitive business information. If your employees have housemates, children, or other family members sharing their space, ask them to consider implementing parental controls to prevent accidental data breaches.

Watch Out For New Big Head Ransomware Pretending To Be A Windows Update!

> *“Big Head ransomware presents victims with a convincing and fake Windows update alert. Attackers design this fake alert to trick users. They think that their computer is undergoing a legitimate Windows update.”*

Imagine you’re working away on your PC and see a Windows update prompt. Instead of ignoring it, you take action. But when you install what you think is a legitimate update, you’re infected with ransomware.

Cybercriminals are constantly devising new ways to infiltrate systems. They encrypt valuable data, leaving victims with difficult choices. One such variant that has emerged recently is the “Big Head” ransomware.

The Big Head Ransomware deception

Big Head ransomware presents victims with a convincing and fake Windows update alert. Attackers design this fake alert to trick users. They think that their computer is undergoing a legitimate Windows update.

The message may appear in a pop-up window or as a notification. The deception goes even further. The ransomware uses a forged Microsoft digital signature. The attack fools the victim into thinking it’s a legitimate Windows update.

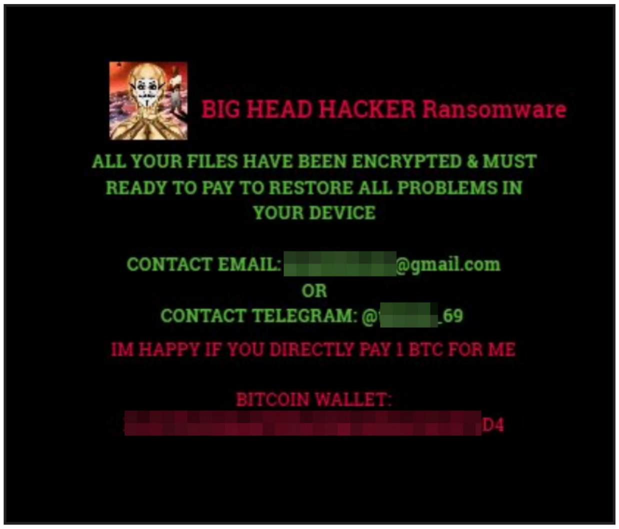
They then unknowingly download and execute the ransomware onto their system. From there, the ransomware proceeds to encrypt the victim’s files.

Victims see a message demanding a ransom payment in exchange for the decryption key.

Here are some strategies to safeguard yourself from ransomware attacks like Big Head:

Keep Software and Systems Updated: Big Head ransomware leverages the appearance of Windows updates. One way to be sure you’re installing a real update is to automate.

Verify the Authenticity of Update: Genuine Windows updates will come directly from Microsoft’s official website or through your IT service provider or Windows Update settings.



BIG HEAD HACKER Ransomware

ALL YOUR FILES HAVE BEEN ENCRYPTED & MUST READY TO PAY TO RESTORE ALL PROBLEMS IN YOUR DEVICE

CONTACT EMAIL: [redacted]@gmail.com

OR

CONTACT TELEGRAM: @[redacted]_69

IM HAPPY IF YOU DIRECTLY PAY 1 BTC FOR ME

BITCOIN WALLET:

[redacted]D4

Backup Your Data Regularly: Back up your important files. Use an external storage device or a secure cloud backup service. Backups of your data can allow you to restore your files without paying a ransom.

Use Robust Security Software: Install reputable antivirus and anti-malware software on your computer.

Educate Yourself and Others: Stay informed about the latest ransomware threats and tactics. Educate yourself and your colleagues or family members.

Use Email Security Measures: Put in place robust email security measures. Be cautious about opening email attachments or clicking on links.

Enable Firewall and Network Security: Activate your computer’s firewall. Use network security solutions to prevent unauthorized access to your network and devices.

Disable Auto-Run Features: Configure your computer to disable auto-run functionality for external drives.

Be Wary of Pop-Up Alerts: Exercise caution when encountering pop-up alerts especially those that ask you to download or install software. Verify the legitimacy of such alerts before taking any action.

Keep an Eye on Your System: Keep an eye on your computer’s performance and any unusual activity. If you notice anything suspicious, investigate immediately.

Have a Response Plan: In the unfortunate event of a ransomware attack, have a response plan in place. Know how to disconnect from the network. Report the incident to your IT department or a cybersecurity professional.

Avoid paying the ransom. In most cases, it is against federal law to pay a ransom to hackers.

Cyber Security Threats Your Team Must Know About

Your employees are your first line of defense in cyber security, and their training is as crucial as the cutting-edge tools you've invested in. Are you overlooking this vital element?

We strongly advise you make an ongoing commitment to regular cyber security training for every single one of your team. That means keeping them up to date on the latest cyber threats, the warning signs to look out for, and of course, what to do should a situation arise.

If you're not already doing that, arrange something now (we can help).

While you wait, here are some urgent cyber threats to address right away:

Admin attack

Email addresses like "info@" or "admin@" are often less protected due to perceived low risk. But several teams may require access to these accounts, making them an easy target. Multi-factor Authentication (MFA) can double your security. Even if it seems tedius, don't neglect it.

MFA fatigue attacks

MFA can feel intrusive, leading employees to approve requests without scrutiny. Cyber criminals exploit this complacency with a flood of fake notifications. Encourage your team to meticulously verify all MFA requests.

Phishing bait

Phishing remains a top threat. Cyber criminals mimic trusted sources with deceptive emails. Teach your team to inspect email addresses closely. Implementing a sender policy framework can also enhance your protection.

Phishing scams are attempts to trick you into revealing your personal information, such as passwords, credit card numbers, or Social Security numbers.

Scammers often send emails or text messages that appear to be from legitimate companies, such as banks, credit card companies, or government agencies. They may also create fake websites that look like real websites.

The three most common phishing scams are:

Fake shopping websites, which sell counterfeit products - or even sell nothing at all. They collect your credit card information to sell to other hackers.

Romance scams to trick people into falling in love, so they'll be more willing to send money.

Social media scams that either impersonate real people, or invent new personas entirely. Other common internet scams include:

Investment scams (yes, people still fall for these every day) that promise victims high returns on their investments, but the investments are actually fake.

Tech support scams which claim to be a tech support company, but then charge for unnecessary services or steal personal information.

Lottery and sweepstakes scams tell people that they have won a lottery or sweepstakes, but they need to pay a fee to claim their prize.

Charity scams impersonate legitimate charities and ask for donations.

Cyber security training doesn't have to be tedious. Try simulated attacks and think of them like an escape room challenge—fun yet enlightening. It's about identifying vulnerabilities, not fault-finding.

Don't exclude your leadership team. They need to understand the response plan in case of a breach, much like a fire drill.

If you receive an email, text, or call from someone who is asking for your personal information or money, be suspicious! Don't click on anything until you verify the sender is who they say they are!

> *"Cyber security training doesn't have to be tedious. Try simulated attacks and think of them like an escape room challenge—fun yet enlightening. It's about identifying vulnerabilities, not fault-finding."*

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Contact Information

Tech Experts
Support Team
(734) 240-0200
support@MyTechExperts.com

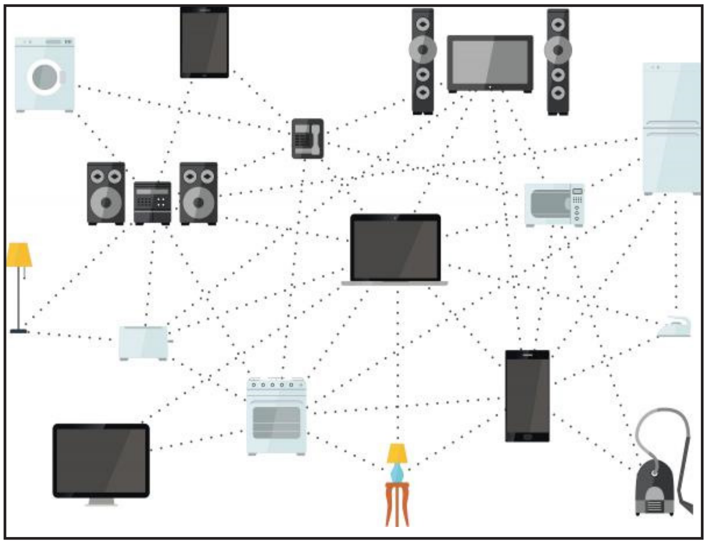
Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Keep Your Smart Home From Turning Against You



Smart homes offer unparalleled convenience and efficiency. But as we embrace the convenience, it's essential to consider the potential risks.

Recent headlines have shed light on the vulnerabilities of smart home technology, such as the story in the New York Post's article titled "Locked Out & Hacked: When Smart Homes Turn on Owners."

The article describes smart home nightmares. Including the new owner of a smart home that unexpectedly got locked in. The prior owner had left preprogrammed settings. Suddenly at 11:30 p.m., the home told him it was time to go to bed and locked every door in the house.

Another technology victim was a woman terrorized by lights and sounds at home. Her ex-partner was maliciously manipulating the smart technology.

As homes get smarter, how can you avoid a similar experience? We'll explore some key strategies to protect your home and your privacy.

Secure your network

The foundation of any smart home is its network. Just as you wouldn't leave your front door wide open, you shouldn't neglect Wi-Fi security.

Strengthen device passwords

Avoid using easily guessable information like "123456" or "password." Use a combination of upper and lower-case letters, numbers, and symbols.

Enable two-factor authentication (2FA)

Many smart home device manufacturers offer 2FA as an extra layer of security. This helps keep unwanted people out.

Regularly update firmware

Firmware updates are essential for fixing security vulnerabilities in your smart devices. Make it a habit to check and apply firmware updates regularly.

Vet your devices

Look for products that have a history of prompt updates and robust security features. Avoid purchasing devices from obscure or untrusted brands.

Isolate sensitive devices

Consider segregating your most sensitive devices onto a separate network, if possible.

Review app permissions

Smart home apps often request access to various permissions on your devices. Before granting these, scrutinize what data the app is trying to access.

Be cautious with voice assistants

Review your voice assistant's privacy settings. Be cautious about what information you share with them. Many devices can be programmed to not listen by default.

Check your devices regularly

Regularly check the status and activity of your smart devices. Look for any unusual behavior.

Understand your device's data usage

Review your smart device's privacy policy. Understand how it uses your data.

Stay informed

Finally, stay informed about the latest developments in smart home security. Subscribe to security newsletters.