August 2021

TechTidbit.com

brought to you by Tech Experts

What's Your Pocket-Sized Security Threat?

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

You guessed it. I'm talking about phones.

How many people in your business have a company-issued phone, or use their own to access company data like emails, client information, or documents? It's probably a high number, right?

And your phone is a big risk to your data security. Smishing attacks (that's the text message equivalent of a phishing email) increased 328% in 2020 and will probably significantly rise again this year.

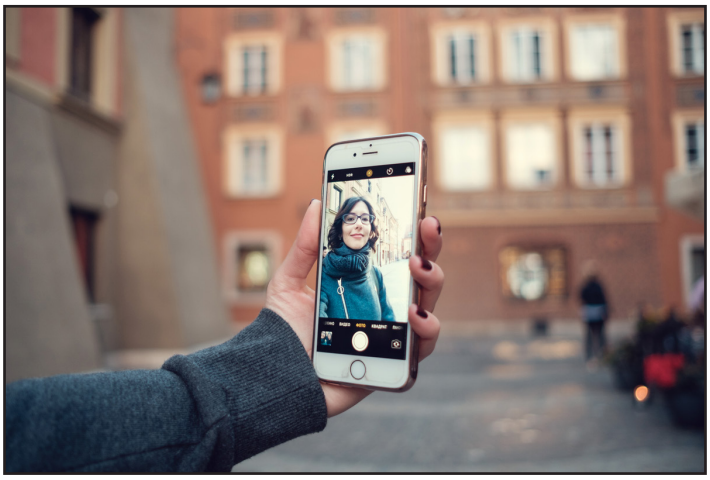
That's because it's a goldmine for cyber criminals. 98% of text messages are read and 45% are responded to. So a smishing text is likely to yield good results for criminals.

Once your phone is infected, malware can monitor your calls and messages, download and delete your data, and if a phone is connected to your business network, the infection might even spread.

Sixty percent of interaction with corporate data happens via a mobile device.

Malware aside, mobile devices are more prone to loss and theft, which could see them easily falling into the wrong hands.

So with all that in mind, what steps are you taking to keep phones protected from threats like cyber-attacks and data theft?



First and foremost, you need to educate your people on the dangers that smart phones pose. Make sure they know how to spot a smishing attempt and not to click or respond to anything that raises a red flag. Encourage everyone to block any numbers sending bad texts, and even consider installing a spam blocking app on all devices.

If your people are in any doubt as to whether a message is genuine or not, ask them to clarify with their contact with a phone call. Don't respond to a message if there is any doubt over its authenticity!

Make sure that everyone uses multi-factor authentication or biometrics to unlock handsets. And set up encryption and the ability to remotely wipe data if a device is lost or stolen.

Everyone in your business should also know exactly what they have to do if they think they've tapped on a potentially dangerous link, downloaded something they shouldn't have, or lost a device. Create a protocol that details who needs to be informed and in what timeframe, the information that needs to be given, and how it's escalated. The sooner a potential breach is reported, the more can be done to quickly rectify the situation and protect your data.

As usual, if you need any further help or advice on keeping all of your devices safe and secure, give us a call.

If your people are in any doubt as to whether a message is genuine or not, ask them to clarify with their contact with a phone call. Don't respond to a message if there is any doubt over its authenticity!

The Internet Of Things Can Poke Holes In Your Network

"You've secured your business network, but what about the smart watches, fitness trackers, connected speakers, thermostats, and every other device with a battery and a tiny signal? Every single one of those devices is a potential inroad to your network."

Mark Funchion is a network technician at Tech Experts.

Some business owners spend a lot of time protecting their network. After putting a firewall in place, configuring security settings, and setting up users with complex passwords (and possibly even 2FA), it's easy to think that's secure enough.

Now, having that solid foundation and framework is great. If you've done that, you're definitely on the right track. But you still might leave yourself open to exploitation without even knowing it.

How does that happen? IoT – the Internet of Things.

You've secured your business network, but what about the smart watches, fitness trackers, connected speakers, thermostats, and every other device with a battery and a tiny signal? Every single one of those devices is a potential inroad to your network.

For example, a user's watch connects to their cell phone, which is connected to your business's Wi-Fi network. With no firewall on the watch, that creates a potential path into your network.

All of these devices require an IP address. In the past, forty people only needed fifty IP addresses to allow everyone to connect their one device to the network, including wiggle room for guests.

Now, every person has a laptop, cell phone, and some sort of accessory – each with its own IP address.

Each of these devices are transmitting a tiny amount of data, but that data and usage grows exponentially.

Plus, if you don't have that wiggle room for extra connections, you're more susceptible to a denial of service (DoS) attack, which is when cybercriminals overwhelm your network with traffic and bring it to a halt.

Your network needs to be able to handle an increase in traffic while also securing all that extra information that you do not have control over.

It is scary and overwhelming, but you can take steps to secure yourself without going too far.

The easy way is withholding access to anything that is not corporate-owned and approved. However, limiting all these devices can have a negative impact on your business and its operation.

Instead, take a measured approach. Make sure your firewall is up-to-date, and monitor who is trying to access your network. Limit that access to the smallest "allow" list you can without making it impossible to work.

For all the smart things like watches and thermostats, keep these IoT devices on a separate virtual network. Encourage and educate users to keep their devices up-to-date – and to use them responsibly while on the network.

Cyberattacks are always increasing and changing, and a strong defense makes a considerable impact when it comes to preventing huge losses in productivity, data, business reputation and funds.

Developers know this too, and that's why it's important that your devices – all of them, from servers and PCs to security cameras and thermostats – are all kept up-to-date. These updates help patch up holes in the firmware and software that can otherwise be exploited.

We're big proponents of the "an ounce of prevention is worth a pound of cure" philosophy. If you need help closing up any gaps in your network security, Tech Experts can assist.

We can conduct a network survey, set policies and passwords, segment and restrict access to/from your network, and ensure the right people have the right access.

As cyberattacks against small businesses mount, the time to fortify your first line of defense is now, before it's too late.

Companies Must Address Employees' Lax Cybersecurity Habits

A third of employees picked up bad cyber security behaviors while working from home, according to Tessian's Back to Work Security Behaviors report.

Despite the remote workers' bad security practices, 9 out of 10 organizations prefer the hybrid workplace as COVID-19 restrictions eased. Similarly, 89% of employees want to work remotely during the week.

The firm advises business owners to consider the bad employee behaviors as organizations transition to hybrid workplace models.

As employees go back to the office, businesses need to address changes to employees' security behaviors since they have been working remotely.

Most employers are wary that the post-pandemic hybrid workforce would bring bad cybersecurity behaviors.

More than half (56%) of employers believed that employees had picked bad security practices while working remotely.

Similarly, nearly two-fifths (39%) of employees also admitted that their employee behaviors differed significantly while working from home compared to the office.

Additionally, nearly a third (36%) admitted discovering 'workarounds' since they started working remotely.

Close to half of workers adopted the risky behavior because they felt that they weren't being watched by IT departments. Nearly a third (30%) said they felt that they could get away with the risky employee behaviors while working away from the office.

However, small businesses placed more confidence in their employees while transitioning to the hybrid workplace.

Over two-thirds of business owners believed that their staff would observe their company's cybersecurity policies.

Many employees are unlikely to admit cutting corners

The fear or failure to report cybersecurity mistakes was a huge cybersecurity risk for organizations. A quarter of employees refused to report such mistakes believing that nobody would ever discover them.

Similarly, more than a quarter feared reporting cybersecurity mistakes to avoid potential disciplinary actions or being forced to take additional security training.

However, younger employees are more likely to admit cutting corners, according to the Tessian report.

More than half (51%) of employees between 16-24 years old and 46% of those between 25-34 years old were more likely to admit circumventing the company's security protocols.

"Create a security culture that encourages people to come forward about their mistakes, and support them when they do," the authors suggested.

Personal devices will undermine the network perimeter in the hybrid workplace

Some of the security threats and challenges experienced when people work fully remotely would be imported into the new hybrid workplace.

While many employees used infected devices for remote access during the pandemic, some would bring them to the hybrid office. Company leaders now have to shift to a new security architecture for good – one that involves zero-trust network access, endpoint security, and multi-factor authentication.

Phishing and ransomware attacks are major challenges in the hybrid workplace

Ransomware attacks were also a major concern for more than two-thirds (69%) of companies who believed that the hybrid work environment would be a target for ransomware attacks. These attacks posed a business continuity threat to targeted companies.

Similarly, phishing attacks concerned over three-quarters of IT decision-makers who believed that credential phishing would only exacerbate in a hybrid workplace.

They believed that employees were more likely to expose company data in public or fall for phishing scams impersonating airlines, booking companies, hotels, or senior executives on a business trip. In fact, "back to work" phishing emails were a concern for 67% of IT leaders.

Phishing was the gateway to ransomware attacks. Consequently, successfully blocking phishing exploits reduces the chances of a ransomware attack.

"Stop phishing, business email compromise, account takeover attacks, and social engineering scams, and you significantly reduce the risk of ransomware," the report authors noted.

However, bad employee behaviors, such as failing to report clicking phishing links, made it harder to stop these attacks.

"While many employees used infected devices for remote access during the pandemic, some would bring them to the hybrid office. Company leaders now have to shift to a new security architecture for good – one that involves zero-trust network access, endpoint security, and multi-factor authentication."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

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

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.

Three Scary Questions To Ask About Your Data On Your Staff's Phones

More and more businesses encourage staff to use their own personal cell to access company data.

It's very convenient and cost effective for everyone. Isn't that the point of having all your data and apps in the cloud? You can access anything anywhere on any device.

But there are downsides. Any time someone accesses business data on a device that you don't control, it opens windows of opportunity for cyber criminals.

Here are 3 scary questions to ask yourself.

What happens if someone's phone is lost or stolen?

What's a pain for them could be a nightmare for you. Would you be able to encrypt your business's data or delete it remotely? Would it be easy for a stranger to unlock the device and access the apps installed?

What happens if someone taps a bad link?

Lots of people read their email on their phone. If they tap on a bad link in a phishing email (a fake email that looks like it's from a real company), is your business's data safe?

Despite what many people think, phones can be hacked in a similar way to your computer.

What happens when someone leaves?

Do you have a plan to block their ongoing access to your business's apps and data? It's the thing many business owners and managers forget when staff change.

If you haven't already, create a cell phone security plan to go with your general IT security plan. Make sure everyone in your business knows what it is and what to do if they suspect anything is wrong.

If you need a hand, don't forget that a trusted IT security partner (like us) can give you the right guidance.

Did you know...

...you can share an exact point in a YouTube video

YouTube

Here's how to share a video so it starts at a specific point.

Sharing videos with colleagues (and friends) is something we do often.

How many times do you think you send someone a video, but they can't be bothered to scroll to the bit you want them to see?

First scroll through the video up to the exact moment you want.

Click 'share.' You'll notice there's a checkbox below the link. Put a tick in that box and the video will start at that exact moment. Easy as that.