May 2020

TechTidbit.com

brought to you by Tech Experts

How To Set Up And Maintain A Secure, Remote Work Environment To Overcome The COVID19 Pandemic

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

"We are in this together." We can't say that enough. It's not you, and I, but US.

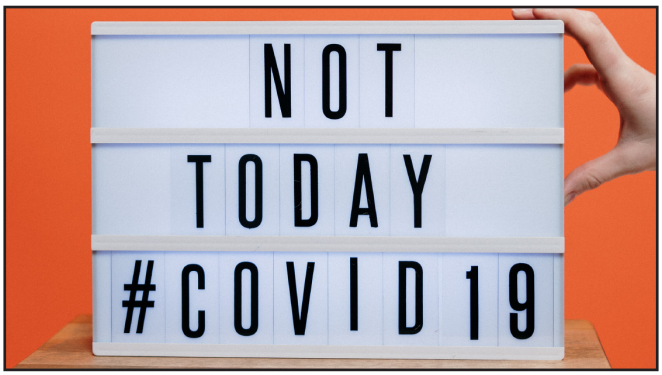
Information technology and communications providers are considered essential services in this unprecedented time, and we take our role seriously. We are here to help, and we ask you (no, implore you) to reach out with any technology-related questions as you work to transition from a central office to a remote employee environment.

As you prepare (or maybe you already have transitioned) for remote work environments, many of which will need to be done by the individual who will be working there, we developed this list of 10 things to keep in mind to secure a remote work environment on the fly.

Invest in antivirus software for all employee devices

Yes, technically it is your employee's devices and these are usually outside of the typical IT circle. But with these circumstances coming about quickly, there may not have been time to follow your normal procurement cycle to get the specific equipment your employees need to remain productive while working from home. That means they will be working from their own device, and they may or may not be as cognizant of your security measures.

So a good rule of thumb is to work to ensure that all employees utilize antivirus software. Many ISPs (Internet service providers) also offer free antivirus software with their service, and we would encourage you to take full advantage. There are several ways you can handle this and we invite you to give us a call to see what will work best for your organization.



Consider VPN security

A VPN is a virtual private network that can provide additional levels of security than the ordinary world wide web. What Is My IP Address shares a great, succinct explanation of VPN:

- A VPN is a service that you sign up for online for a small monthly charge.
- Once you have an account, your VPN service should be "on" when you're online.
- A VPN, in action, takes your Internet connection and makes it more secure, helps you stay anonymous and helps you get around blocks and access censored sites.
- The key to a VPN is that it lends you a temporary IP address and hides your true IP address from every website or email you connect with, protecting your private network.

Provide support for setting up a secure home network

Here is where we come in. During this time, invite your staff to reach out to us directly to help your employees troubleshoot any challenges they may have when setting up their home network and effectively securing it. To maintain consistency it may be in your best interest to provide standard routers and equipment (if feasible) to all of your newly remote employees so you can ensure that all users are utilizing the same technology and security protocols.

Train Employees on Effective Physical Security Measures

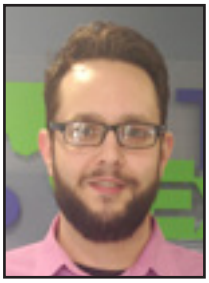
Brian Stark, general manager of North America at smanos, a smart home and DIY security company told Business

Continued on page 4

Now is the perfect time to evaluate who has access to what programs and files. You might find that some who had access did not necessarily need it or use it, and that license can be moved to another. With many software solutions being subscription-based, this could end up being a cost-saving measure in these unique times.

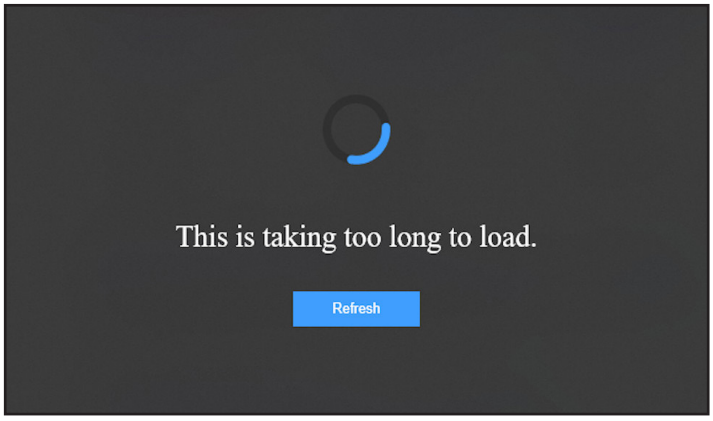
Did Your Windows 10 Search Function Break?

"In terms of a Microsoft turnaround, a 1-day fix is quite incredible. Some users experienced it for a bit longer as the fix was not always applied automatically. The problems were sporadic, but some machines took a few restarts to apply the hotfix."



Jason Cooley is Support Services Manager at Tech Experts.

It seems like every time I turn around I have a new Windows 10 story to share. The combined abundance and variety of issues has been frustrating to say the least. The number of users affected normally varies as people will install updates at different times, but those updates are the most likely cause of a widespread issue.



Microsoft recently had one of the most widespread issues in its Windows 10 OS history, and that is quite a statement. It likely affected more users than any group on a given operating system version.

When trying to update something in its own programming for Windows 10, Microsoft broke the search feature.

First, some background information: Windows 10 search is built-in and Microsoft has integrated the search with Bing to allow for both local searching of your system and online results as well.

The option can be very useful for users as it allows a centralized location to look for whatever you might need to find. Personally, I still use the search feature for Windows functions and use Google to do any web searches. That said, I can see the value the search feature has for some.

For each person it works well for, there is a user that will search for something on their computer then accidentally open a Bing search result for something they never had any intention of opening.

It happened recently to someone I know. They were searching for their scanner and nearly downloaded a third party application from an untrusted source. It can happen easily and frequently.

Whether you find use in local and online results or you are more like me and use the search purely for Windows functions, you likely rely on it to some degree.

So what would you do if you had no ability to search at all? What if the entire functionality of searching was broken in Windows 10? That is what happened recently to just about every person who happened to login over a few day period recently. Microsoft was updating some of its backend search code (likely making changes to Bing itself) and didn't account for an impact on the integrated search.

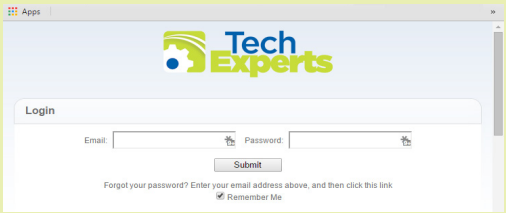
The impact on each user varied, but even as someone who is very comfortable using Windows 10, the broken search function really made things more difficult. Fortunately, the problem was very quickly resolved.

In terms of a Microsoft turnaround, a 1-day fix is quite incredible. Some users experienced it for a bit longer as the fix was not always applied automatically. The problems were sporadic, but some machines took a few restarts to apply the hotfix.

When you break Windows for almost all of your users (especially right after taking away the most loved operating system of all time), fixing it quick is in your best interest. That is exactly what Microsoft did. Let's just hope we all achieve a little stability now that some of their resources have been freed up with the end of Windows 7.

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



Email Checklist: Is It A Phishing Attack?

More than half of phishing attack emails contain malicious links. Furthermore, approximately one-third of all phishing attack emails manage to bypass default security methods.

So how do you determine if an email you've received is aphishing attack?

Sure, sometimes it's obvious. But as cybercriminals continue to evolve and become more sophisticated, their phishing attack emails are becoming more convincing than ever before.

Here's a complete checklist to go through when you receive a suspicious email:

An Overly Generic Greeting

More often than not, phishing emails are sent out to a massive list rather than one individual.

This means they'll often contain generic greetings, such as "dear customer" or "dear member" whereas a legitimate source, such as your bank or a government organization, would probably address you by name.

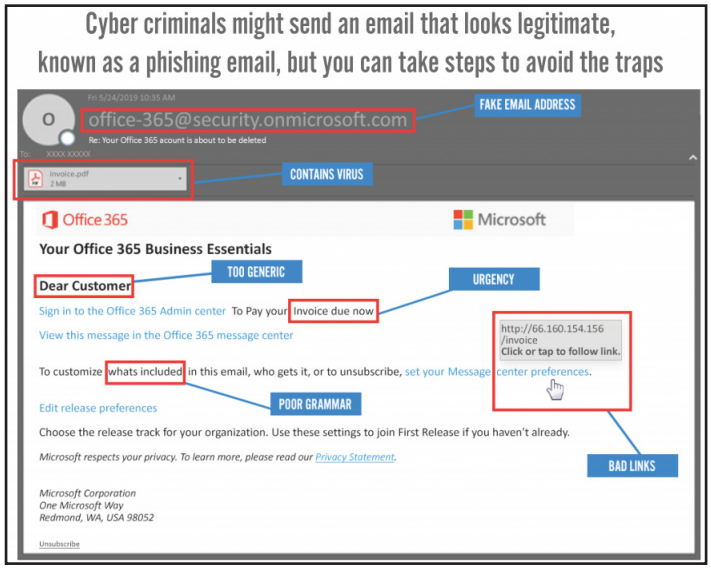
A Request to Update or Verify Information

If the email contains some sort of request to update or verify your information, it's likely a phishing email. No legitimate source will ask you to update or verify sensitive information over the internet. Chances are, they will call you or wait until you're in the store/at the bank to go over this request with you.

A Lack of a Domain Address

Aside from looking at the name and company information, don't forget to double check their domain address.

Hover your mouse over the "from" address to see if there is a legitimate domain or not. For instance, they may have !IRA.com instead of IRA.com. However, this isn't always foolproof and it's important to check for other signs too.



Grammar and/or Spelling Errors

Large organizations tend to spell check their email content carefully - meaning it's not very common to find grammar and/or spelling errors throughout emails from your bank, government entities and other legitimate sources. Pay close attention to the grammar and/or spelling in the email.

A Sense of Urgency

If something is urgent, a legitimate source will typically call you or send you a piece of direct mail.

Cybercriminals tend to create a sense of urgency, such as "if you don't respond, your account will be canceled" or "if you don't pay the attached invoice, you will be charged interest and it will go to collections."

An Unsolicited Attachment

As a general rule, if the email contains an unsolicited attachment from an unknown sender or an unsolicited attachment that seems out of place from a sender you do know, don't open it.

Typically, legitimate sources don't randomly send emails with attachments. Instead, they will direct you to download something directly from their website.

Suspicious Links

Before you click on a link, hover over it to see where the link is actually going to take you. Often, cybercriminals will make it appear as though the link is going to a legitimate place, but once you've hovered over it, you'll find that it's taking you to somewhere else entirely. Always hover over any links before clicking them.

"Before you click on a link, hover over it to see where the link is actually going to take you. Often, cybercriminals will make it appear as though the link is going to a legitimate place, but once you've hovered over it, you'll find that it's taking you to somewhere else entirely. Always hover over any links before clicking them."

How To Set Up And Maintain A Secure, Remote Work Environment To Overcome The COVID19 Pandemic, continued

News Daily that, "Home offices often contain expensive equipment or even physical files or documents that contain sensitive information, so it's imperative to explore security options. While it's not possible for all home offices to have a scan-to-enter system or a security guard, it's important to add whatever elements of traditional physical security you can."

Just being aware of your physical surroundings can be critical in maintaining physical security. And another rarely thought of aspect to securing a home office is family.

While they may not have malicious intent in mind, files can accidentally be deleted, or accidental e-mails sent. So, encourage your employees to keep family off of their devices, especially unsupervised.

Clearly and regularly communicate company policies

You have clear rules for technology inside of the office, so you should also have specific policies for home offices. While you can't police as strictly as you could within the office, you should still develop a specific list of requirements your employees should follow such as:

- Regular scanning of the device for malware and viruses.
- Timed screensaver automatically locking down the desktop if away for a certain amount of time.
- Hours the employee is expected to be available.
- Allowed business communications platforms, such as Slack, or Microsoft Teams.

In addition, you also need to clearly communicate to your employees the reporting process and requirements if they do find themselves infected with a virus or malware so that you can react proactively to any potential threat.

Use a centralized storage solution

If you haven't already, you will want to decide on a centralized storage solution. Whether you chose a cloud solution or an on-premise solution, now that your employees are working outside of the office, having a centralized storage solution can ensure you retain access to any and all of your employees' work product. Andrew Hay, chief information security officer at DataGravity, explains the importance of this with Business News Daily, stating that "Ensuring that sensitive data is stored and protected centrally is always a good course of action.

This allows central management and control of all aspects of the data, such as ownership, access, availability, security, etc., with a reduced chance of duplicate copies residing in places beyond the reach of the organization, such as on a personal laptop, mobile device or cloud environment." And, in the event that an employee needs to be let go, you can ensure access to the items that the employee was personally responsible for.

Enforce reasonable session time-outs for sensitive programs or applications

Employees step away from their desks. It happens. Bathroom breaks, to grab another glass of water or lunch. The essential cup of coffee. But timing-out within seconds of inactivity can lead to frustration as workers must keep reloading programs.

A session time-out is a necessary security process, as not everyone always remembers to log out at the end of the day, but be sure that you set the time-out for a reasonable amount of time.

Limit file access to only the areas absolutely needed by the employee

Now is the perfect time to evaluate who has access to what programs and files. You might find that some who had access did not necessarily need it or use it, and that license can be moved to another. With many software solutions being subscription-based, this could end up being a cost-saving measure in these unique times.

Reserve the right to terminate employee access at any moment

Unfortunately, there are times that employees need to be let go or events where an unauthorized individual gains access to their physical device. If you notice suspicious activity on a particular employee's account, don't hesitate to turn it off, even before speaking with the employee.

Moving forward in this temporary new normal

Our worlds have been turned upside down by the events that have taken place these last few weeks and we all are working to pivot and find our feet in this new normal. We are all in this together, and together we can secure your future for when this current time is over. What was once considered normal may not be normal tomorrow.

So, what is the "new normal" these days?! Notice, some businesses are moving to working from home, doing video teleconferencing calls and having virtual networking events… This has become the new normal. If your business is adjusting to COVID-19 and you need help migrating your staff or training them on how to properly use video teleconferencing software, we can help. Do not hesitate to reach out.

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