QUESTION

Can my phone be hacked?

ANSWER

Yes! As well as the risk of phishing and smishing (that's phishing via text message), you also put your data at risk by connecting to public Wi-Fi. Fake apps can also be an issue.

QUESTION

How can I make my display more organized?

ANSWER

Consider adding a second monitor. Not only will this allow you to better organize your apps and windows, but it will also give you more workspace.

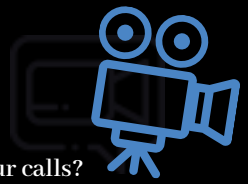
QUESTION

How do I know if my Teams app is up to date?

ANSWER

Just click on the three dots next to your profile picture and select 'Check for Updates' from the menu. If you're using Windows 11, you'll need to check under Settings -> About Teams.

YOUR NEXT STEPS...



Ask yourself these questions:

1. Am I 100% happy with our IT provider's responses to our calls?
2. Am I 100% certain that our current IT provider has us fully protected from any disaster?
3. Am I 100% confident that our IT provider is proactively helping us achieve our business goals?

If you're not 100% sure, let's schedule a 15-minute call. No sales pitch, we promise! We just want to get to know you and ensure that your IT investment is getting you the results that you deserve.

Email us at info@durham-it.ca or book a call at https://www.durham-it.ca/book-a-call/.

September 2022

Durham IT's Tech Tips For The Boss

Your monthly newsletter, written for humans not geeks

Did You Know?

You might have a RAT?

Malware gets some funny names and acronyms. One you might have heard of is the RAT – which stands for Remote Access Trojan.

It's okay when your IT partner accesses your computer remotely, as you can watch what they're doing. But with a RAT, cyber criminals have secret remote access and you have no idea that they are in your system. They can watch what you're doing, copy your passwords and launch a ransomware attack.

The simplest way to avoid a RAT is to never download files from sources you don't trust, or open email attachments from strangers. Make sure your business has appropriate cyber security software and regular training for your team.

www.linkedin.com/company/durham-it www.facebook.com/durhamits
www.durham-it.ca

Your Remote Workers Aren't Using Computers That Look Like This, Are They???

When did you last check that everything was up to par with the devices your remote workers are using?

That might sound like a strange question, but we recently discovered that 67% of remote workers are using faulty devices at home.

Now, why would they do that? They've likely damaged the device themselves and are too scared to tell you!

Laptops, keyboards, and monitors are most likely to be damaged (in that order), and it's most often because of food or drink spills... though some people blame their partners, children, and even their pets! We've all watched in horror as a cat rubs itself against a full glass of water next to a laptop...

Using a device that doesn't work properly is a problem, of course. First, it's going to damage your team's productivity. Tasks might take longer or be more difficult to complete. If they try to fix the problem themselves, they risk causing further damage.

No... a fork isn't a clever way to get bits of cake out of your keyboard...

But the other issue is that of security. In some cases, your people will stop using their damaged company-issued device, and use a personal device instead.

This puts your data at risk because their personal devices won't have the same level of protection as your business devices.

It also means that if they're connecting to your network, it might not be a safe connection, potentially leaving the door open for cyber criminals.

Also, because your IT partner isn't monitoring personal devices, it's possible they won't spot an intrusion until it's too late.

Our advice? Make it a regular routine to check that everyone's happy with their devices. You should also have a policy that they won't get in trouble for accidental damage, so long as it's reported immediately.

If you need help replacing any damaged devices, just give us a call.

Malware is Becoming Increasingly Difficult to Spot

According to new research, four out of five malware attacks delivered by encrypted connections evade detection. Since two thirds of malware is now arriving this way, this has the potential to be a big problem for your business.

This type of threat has already hit record levels and continues to grow. So, if you don't yet have a response and recovery plan in place, now's the time to create one.

This plan works alongside your cyber security software protection and regular staff training. The plan details what you do in the event of a cyber-attack.

Having the right plan in place means all your people will know how to sound the alarm if something is wrong. It ensures downtime and damage are kept to an absolute minimum.

The faster you respond to an attack, the less data you should lose and the less it should cost you to fix things.

Of course, you should also follow the usual security guidelines of making sure that updates and patches are installed immediately, and you are regularly checking your backup is working and verified.

Businesses that don't place a high importance on their own cyber security planning are the ones hit hardest by such an attack.

Can we help you create your response and recovery plan? Call us.

DURHAM IT SERVICES

www.durham-it.ca

CALL: 905-231-1303 | **EMAIL:** info@durham-it.ca