
**QUESTION**

I know I just saved a document, but I can't find where it went.

**ANSWER**

This is more common than you think. You click 'save' and when you try and reopen your file, it's not in the folder you thought you saved it to. Don't worry, simply open up a folder, click on 'recents' and your document should be there. Look at the file information and it will show you where you've saved it.

**QUESTION**

My apps keep crashing, what's wrong?

**ANSWER**

In true IT support style: have you tried turning your device off and on again? If it's still happening, try deleting the app and reinstalling it. If it's still happening, you may be low on storage space.

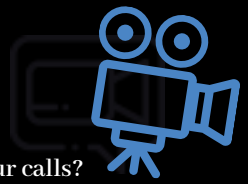
**QUESTION**

I clicked a link in a phishing email. What do I do?

**ANSWER**

First, do not enter any data. Disconnect your device from the internet. If you've got malware, this will stop it from spreading. Run a full malware scan and consult an IT expert. They'll advise how safe your backups are, and whether you need to change any passwords.

## 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/.**



March 2022

# Durham IT's Tech Tips For The Boss

*Your monthly newsletter, written for humans not geeks*

## Did You Know?

**Did you know... you don't need a third party app to screen share?**

If you've ever found yourself teaching older members of your family how to use Zoom, you'll understand the frustration of trying to explain something without being able to see what the other person can see. In these cases, screen sharing can be very helpful.

However, downloading a third party app to do this isn't always straightforward, and it relies on the other person being able to do the same.

Here's the answer... did you know you can use Quick Assist on Windows PC? Just type 'quick assist' in the taskbar. You'll be given two options: 'Give assistance' and 'Get assistance'. Select the one you need and simply follow the instructions on screen.

A word of warning: only allow this kind of access to your device to someone you know and trust.

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

# ONE WAY OR ANOTHER, YOUR PEOPLE ARE GOING TO TAKE YOUR BUSINESS DOWN

**The threat of an insider attack in your business is more real than you realize.**

**Of course, it's not always intentional. Most insider attacks happen because of naivety or negligence. Perhaps you haven't educated your people on cyber security and the red flags to be aware of. Or maybe someone had a momentary lapse in judgement. It happens... a lot.**

**But almost a quarter of insider attacks are malicious.**

**That means that someone on the inside is actively stealing your data, or allowing others access to it. This may be someone with a grudge, someone looking for financial gain, or even someone who has already left the business.**

**So what plans do you have in place to tackle and reduce your risk of an insider attack? As with everything in business, planning is the best way to get ahead. With the estimated cost per insider attack being hundreds of thousands of $$$, can you afford not to create a plan to protect your data?**

**We call this an insider threat strategy, and it covers everything from training to staff exit planning.**

**For a short time, we're offering to create an insider threat strategy for local businesses. Our experts will assess your business, its current security measures, and make recommendations to keep your data safe.**

**Visit www.durham-it.ca/book-a-call/ to book a 15 minute no obligation video call.**

# Let's Ditch the Passwords...

Don't panic, we haven't gone completely crazy. We are still the security-conscious company you know and love.

But passwords are a pain:

- First it was "remember to change your password frequently"
- Then it was "use randomly generated passwords"
- And then "don't forget to use a password manager"

Things change so often that it's become hard to keep up. However, we're lucky that we're being given new, more secure ways to keep our people and data protected.

With biometrics becoming more widely used, it's time you make some more changes to the way you log into your devices.

What are biometrics? You may already be using them – it's when you use facial or fingerprint recognition to unlock your device. Retinal scanning is even a thing, although not yet widespread for everyday devices. They give you an added layer of security because someone can't steal your fingerprint or your face!

You can also use biometrics across your apps and software to give you more protection from cyber criminals. It means that should someone steal your device or access it remotely, they can't access your accounts and data. What better way is there to protect your accounts?

If you haven't got biometrics set up within your business, give it a try. We can guarantee that this technology is only going to increase in popularity thanks to the added protection it gives you.

DURHAM IT SERVICES

www.durham-it.ca

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