November 2021

TechTidbit.com

brought to you by Tech Experts

If You've Ever Reused A Password To Sign Up For Something New, You Have A Problem…

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

It's something many people admit to doing: they reuse the same password across a few different services.

Not judging you if you've done it. It's easy to see why thousands of people do this every day. It feels like an easy way to get signed up to something.

If you reuse a password, you won't have to go through the hassle of trying to remember it and needing to reset the password in the future. However, you only have to do this once, and you're at big risk of something called credential stuffing.

This is where hackers get hold of millions of real usernames and passwords. These typically come from the big leaks we hear about in the news.

Once leaked, information from databases from major companies like FaceBook, Twitter and LinkedIn can be bought on the dark web for pennies each.

And then they try all those details to see if they can login to other digital services. They use bots to stuff the credentials into the login box, hence the name.

Because it's automated, they can sit back until their software manages to log into an account… and then they can do damage or steal money. Stats suggest that 0.1% of breached credentials will result in a successful login to another service.

The best way to protect yourself against this kind of attack is to never, ever reuse passwords.

Use a password manager to generate long random passwords, remember them for you, and auto-fill them. You only have to remember the password for your password manager.

The less hassle for you, the less likely you are to reuse a password. Consider giving a password manager to each of your staff as well.

And if you know you have reused passwords in the past, then you should really change all your passwords on all active services.

Once leaked, information from databases from major companies like FaceBook, Twitter and LinkedIn can be bought on the dark web for pennies each.

A Quick Refresher On How To Keep Your Business Safe

If you connect it, protect it

As more and more technology becomes a part of our personal and business lives, the line between our online and offline self has become increasingly blurred. Stay Safe Online reminds us that any device we connect to our home and business network needs to be protected and each has some amount of risk associated with the connection. So all of our smart thermostats, TVs, doorbells, alarm systems, and refrigerators, need to have the appropriate protection policies in place.

Securing devices at home and at work

The global pandemic has removed the boundaries between "home" and "work" as much work was completed while at home. Remote work was already well on it's way to becoming the new normal of work the adoption of the strategy was accelerated. With devices connecting from both our home and our physical workspace, this has opened the doors to a different kind of cybersecurity concern and how you can protect both.

Securing Internet-connected devices in healthcare

More and more healthcare facilities, from senior living to urgent care centers, are using Internet-connected devices in the day-to-day care of their patients. Tele-medicine has quickly emerged as a way for patients to receive care and doctors to give it as a result of COVID-19, but this opens both patients and providers to unique cybersecurity challenges. Strong passwords and encrypted Wi-fi will help to keep data secure.

Outdated Software Could Cost Much More Than An Upgrade

"If you know the software inside and out, so do the hackers. It's far easier for them to utilize a known flaw than attempt to break a new and unknown software. The longer you wait to update, the more likely it is that your data or network will be compromised."

Mark Funchion is a network technician at Tech Experts.

It's nice when we own something and it's completely paid for. Think of a car or large purchase you financed. Once it's paid off, you feel great: money is freed up and it's yours.

However, often in these situations, you've poured a few years of use into it by the time it's paid off. When something finally breaks, the warranty has probably already expired. Then, you're forced to decide if you are going to put money into this old car or appliance or if it's time to upgrade instead.

When you don't upgrade your car or appliances, there may be some small risks in terms of missing out on improved safety or the newest features, but the biggest risk will be monetary.

Businesses sticking it out with old software isn't much different, but the consequences can be much worse.

Software is sometimes pricey, and often, the outdated software will still technically work. We get used to the layout and processes, and it becomes easy to use. After five or ten years, you know where all the buttons are. Your documentation for employees might be based this particular version, and you may not have the time to overhaul your reference materials.

The issue with this is, while you're happy to run the 2015 version of a software, that software company has released a new version in 2016, 2017, 2018, etc. Usually, they will still update old versions for a short time after new ones come out.

Once these software companies stop providing updates, however, any known vulnerabilities will remain unpatched and any new vulnerabilities that are discovered will not be addressed.

If you know the software inside and out, so do the hackers. It's far easier for them to utilize a known flaw than attempt to break a new and unknown software. The longer you wait to update, the more likely it is that your data or network will be compromised.

Yes, paying for that new version of software is not something we want to do, but in the long run, it may save you a lot of money and headaches.

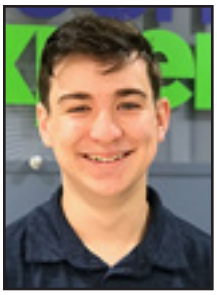
Software as a Service (SaaS) also makes this a little easier to deal with. Rather than paying a huge amount one time upfront, you can often subscribe and pay a smaller amount monthly or yearly that allows you to install new versions as they come out. This usually includes security patches and updates too.

Another consequence of holding out on updating old software is the possibility that your PC may need to be suddenly replaced or updated. If it crashes or becomes too slow to reliably use, you can lose that program. A lot of software is provided via download, and it may not be available for download once it's time for a new PC.

In addition, if you bought something that was written for Windows 7 and have not upgraded in the past six years, it may not be possible to use that program if you are stuck five versions behind. Also, since you paid the vendor long ago, they often won't help you reinstall the old software; instead, they'll require you to buy a current version before assisting.

We understand that staying with what you're familiar with is easy. Since you own the software, it carries a financial benefit as well. However, the short-term financial gains risk data loss and essential parts of your business becoming unrecoverable in a disaster. Look at software updates like insurance: you are paying to keep yourself as protected as possible and working to minimize any potential risk.

Using Technology To Maximize Your Business' Efficiency and Communication



Wyatt Funchion is a tech support intern at Tech Experts.

In today's world, we have so much technology that we barely know what half of it does, let alone how to use it. We tend to stick to what we know and forgo the rest. However, once you understand how you can optimize the relevant tech in your business, you can radically improve efficiency and communication.

One easy way to increase your business' efficiency and keep everyone on the same page is by using a group-based calendar.

Staff can see what the plans are for the day, who's going to be out of the office, schedule meetings and appointments, and more. Everyone can plan their day around each other's availabilities and come in every day knowing what to expect.

Shared drives, either on a network or through a hosting service like OneDrive for Business, can also save time and increase work efficiency.

Shared folders and drives can be divided by department (like Marketing) or use (like Scanned Documents), ensuring files can be accessed instantly in their current version by all allowed parties. You can also filter out who has access to certain folders.

If it would be a right fit for your business, it might be worth looking into a customer relationship management (CRM) system.

A CRM system does what it sounds like: it tracks your relationships with your clients. It does much more than digitize your client files; these are a powerful tool that can do a lot of heavy lifting in organizing your business, managing your clients and workload, marketing, collaboration between employees, and client satisfaction.

There are many, many webpages written on the topic and many CRM options to choose from at all different price points, so some independent research will benefit you here.

We use a CRM program at Tech Experts to track all of our clients' service tickets, manage invoicing, build marketing campaigns, monitor statistics, and more.

Back to the tech that's easier to implement. If you use a fax line, you may be able to switch to an email-to-fax/fax-to-email service or an online fax service.

These solutions function just like a regular fax line (make sure the provider you're considering is HIPAA compliant, if needed) and are often cheaper than a traditional fax machine when compared. These faxes can be sent from anywhere, to multiple parties at once, and save on paper and equipment costs.

Many companies, including ours, use an online library (also known as a knowledge base) to store employee training and reference materials.

This makes it easy for both new and established employees to check procedures without having to interrupt another employee; they simply log in and find the article they need to complete their task.

Additionally, if someone does need to ask for help, they can be directly linked to detailed processes, saving time for everybody involved.

These also allow you to control who has access to what spaces. Services like this are typically browser-based, but something similar could be set up on shared network drives as well.

With the amount of people that are currently working remotely or people who will be working remotely in the future, communication is key.

Not only can these help with communication inside of your business, but also assist in communication with your customers.

"Many companies, including ours, use an online library (also known as a knowledge base) to store employee training and reference materials. This makes it easy for both new and established employees to check procedures without having to interrupt another employee; they simply log in and find the article they need to complete their task.

The Biggest Cyber Threat To Your Business Is In Your Pocket

According to a Verizon study, one in three businesses has admitted to suffering a breach as a result of a mobile device. The same study found that 80% of businesses were aware that they had a big gap in their network security as a result of mobile device usage.

Banning the use of mobile devices for work is not an option, however. The productivity benefits of these mobile devices are too big to give up, and chances are, employees will still use them.

So how can you make sure that your data is safe as it travels around in your (and your employee's) pockets?

Basic protection for all operating systems

Regardless of your operating system and device model, the following security protocols can easily be implemented.

Fingerprint and/or face recognition and secure passcode - this feature not only protects you, but your employee as well. Highlight and encourage employees to set this security feature up on their devices.

Offer internal support to help less tech-inclined employees to set this up and troubleshoot common challenges with unlocking the device with these features.

Not only will this help keep your information secure if the device is lost, but it will also help prevent other unauthorized individuals from accessing your device if it is left unattended.

Use a VPN - A VPN provides a secure phone connection to a private server between your devices and your data and bypasses using public networks to access your information. This helps secure the data and encrypts it as it travels from point to point.

Enable data encryption - Both Android and iPhone devices can be encrypted through the device and it is highly recommended that you encourage your employees to activate this feature. Spreadprivacy.com has detailed instructions on how to do this for both Android and iPhone devices.

Set up remote wipe capabilities - Depending on the device, there is a function along the lines of Find My Phone that you can have implemented that will allow you to remotely lock and erase the device in the event it is lost or stolen.

Apple devices have the function built into the operating system and Android devices can enable this feature with app downloads.

Mobile protection for Android users

One of the great things about Android devices is that you have a variety of manufacturers, features, and price points to choose from.

While they might differ slightly in features and functionality, here are some basic tips for protecting your Android device:

- Only buy Androids from vendors who are proactive in issuing security patches
- Use 2FA (Two-factor authentication)
- Take advantage of built-in security features
- Do not save all passwords
- Only buy apps from Google Play
- Always, always back up the device's data
- Encrypt your device (See instructions above)
- Be careful about connecting to public WiFi, and be diligent about securing your own WiFi networks.
- Use the Android security app
- Install a VPN

Mobile protection for iPhone users

Regardless of the model, all Apple iPhone devices will have the following security features. Keep in mind, however, that older models of the phone will not be able to take advantage of the newest iOS and may require an upgrade.

Here are 10 tips for keeping your iPhone safe:

- Update the iOS frequently. You can opt into automatic software updates through your phone as well so you don't have to keep an eye out for new updates
- Enable 2FA (Two-factor Authentication)
- Set the phone to "self-destruct" or wipe the entire phone after someone fails to access the phone 10 times.
- Activate "Find my iPhone.
- Avoid public WiFi
- Only use trusted iPhone charging stations
- Change your iTunes and iCloud passwords regularly.
- Revoke permissions to your camera, microphone, etc
- Use a passcode longer than 4 numbers
- Disable Siri access from the lock screen.

Take the next step

These tips will get you started on keeping your business, and personal, information safe as you roam. But this is just the first step. Take the next step and set up a full security audit to see where there may be a crack in your armor that leaves you vulnerable.

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