May 2024

TechTidbit.com

brought to you by Tech Experts

# How To Make The Pain Of Passwords Go Away

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

Passwords. They're the keys to our digital kingdoms, but also the biggest pain in our necks.

They've been around since the dawn of the internet, and guess what? Even with replacements being introduced, they're not going away anytime soon.

I'm sure you've felt the pain of managing a billion passwords for all your accounts. It's exhausting and risky. Perhaps it's time you considered using a password manager.

The real beauty of password managers is you only have to remember one password – the master password to log in to your manager. Then, it does everything else for you.

- It creates long random passwords
- It remembers them and stores them safely
- And it will even fill them into the login page for you

That means no more wracking your brain trying to remember if your password is "P@ssw0rd123" or "Pa55w0rd123" (both are really bad and dangerously weak passwords, by the way). With a password manager, all the work is done for you.

We won't sugar coat it – password managers aren't invincible. Like all superheroes, they have their weaknesses. Cyber criminals can sometimes trick password managers into auto filling login details on fake websites.

But there are ways to outsmart criminals.

First, disable the automatic autofill feature. Yes, it's convenient, but better safe than sorry, right? Only trigger autofill when you're 100% sure the website is legit.

And when choosing a password manager, go for one with strong encryption and multi-factor authentication (MFA) where you generate a code on another device to prove it's you.

These extra layers of security can make a big difference in making your accounts impenetrable.

Enterprise password managers offer useful features like setting password policies and analyzing your teams' passwords for vulnerabilities. Plus, they often come with behavior analysis tools powered by machine learning tech. Highly recommended.

But here's the thing – no matter how advanced your password manager is, it's only as good as the person using it. So, do yourself a favor: Train your team to stay vigilant against scams, and always keep your password manager up to date.

We can recommend the right password manager for your business and help you and your team use it in the right way. Get in touch at (734) 457-5000, or info@mytechexperts.com.

The real beauty of password managers is you only have to remember one password – the master password to log in to your manager. Then, it does everything else for you.

# You'd Be Lost Without It, So Don't Forget Email Security

*"In fact, small and medium-sized businesses are often seen as easier targets. That's because they may not have the same level of security measures in place as larger corporations."*

Let's talk about something super important: Email security. Yep, we know it might not sound like the most thrilling topic, but it's a big deal. Businesses like yours face more cyber threats than ever.

We've seen our fair share of cyber attacks, and let us tell you, many of them start with a simple email (official figures say it's a massive 90%!). Yep, that innocent-looking message in your inbox could be the gateway for cyber criminals to wreak havoc on your business.

So, why is keeping your business email secure so important? Well, for starters, it's your first line of defense against cyber attacks. Think of it like locking the front door of your house to keep out intruders.

If your email is secure, you're making it a whole lot harder for cyber criminals to sneak in and steal your sensitive data.

But implementing proper email security measures safeguards your valuable data from getting lost or falling into the wrong hands.

It's not just cyber criminals you're at risk from; an employee could accidentally leave a laptop on a train or in a coffee shop.

That could mean all your important business communications and documents were suddenly open for someone else to read. It would be a nightmare, right?

You might be thinking, "But I'm just a small business. Why would I be a target?" Ah, but here's the thing – cyber criminals don't discriminate based on business size.

In fact, small and medium-sized businesses are often seen as easier targets. That's because they may not have the same level of security measures in place as larger corporations.

So, don't think you're off the hook just because you're not a Fortune 500 company.

Now that we've established why email security is crucial, let's talk about how you can ramp up your defenses.

First off, use strong, unique passwords for your email accounts. None of that "p@ssW0rd123" nonsense, please.

Better still, use a password manager to create and store uncrackable passwords.

Consider implementing two-factor authentication for an extra layer of security (where you generate a login code on another device to prove it's you).

And don't forget to keep your software and security patches up to date – those updates often contain important fixes for vulnerabilities that cyber criminals love to exploit.

Lastly, educate your employees about the importance of email security. They could be your strongest defense or your weakest link when it comes to keeping your business safe from cyber threats.

Teach them how to spot phishing emails (emails pretending to be from someone you trust) and what to do if they suspect something isn't right.

Remember, a little prevention now can save you a huge headache, time, trouble (and money) later. If we can help with that, get in touch.

## We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

# Google & Yahoo's New DMARC Policy - Why Businesses Need Email Authentication

Have you been hearing more about email authentication lately? There is a reason for that. It's the prevalence of phishing as a major security threat. Phishing continues as the main cause of data breaches and security incidents. This has been the case for many years.

A major shift in the email landscape is happening. The reason is to combat phishing scams. Email authentication is becoming a requirement for email service providers. It's crucial to your online presence and communication to pay attention to this shift.

Google and Yahoo are two of the world's largest email providers. They have implemented a new DMARC policy that took effect in February 2024. This policy essentially makes email authentication essential. It's targeted at businesses sending emails through Gmail and Yahoo Mail.

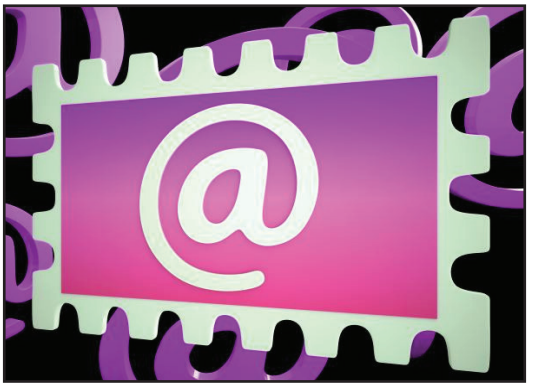
But what's DMARC, and why is it suddenly so important?

## The email spoofing problem

Imagine receiving an email seemingly from your bank. It requests urgent action. You click a link, enter your details, and boom – your information is compromised. The common name for this is email spoofing.

It's where scammers disguise their email addresses. They try to appear as legitimate individuals or organizations. Scammers spoof a business's email address. Then they email customers and vendors pretending to be that business.

These deceptive tactics can have devastating consequences on companies. These include:



- Financial losses
- Reputational damage
- Data breaches
- Loss of future business

Unfortunately, email spoofing is a growing problem. It makes email authentication a critical defense measure.

## What is email authentication?

Email authentication is a way of verifying that your email is legitimate. This includes verifying the server sending the email. It also includes reporting back unauthorized uses of a company domain.

Email authentication uses three key protocols, and each has a specific job:

- SPF (Sender Policy Framework): Records the IP addresses authorized to send email for a domain.
- DKIM (DomainKeys Identified Mail): Allows domain owners to digitally "sign" emails, verifying legitimacy.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Gives instructions to a receiving email server including, what to do with the results of an SPF and DKIM check. It also alerts domain owners that their domain is being spoofed.

SPF and DKIM are protective steps. DMARC provides information critical to security enforcement. It helps keep scammers from using your domain name in spoofing attempts.

## Why Google & Yahoo's new DMARC policy matters

Both Google and Yahoo have offered some level of spam filtering but didn't strictly enforce DMARC policies.

Starting in February 2024, the new rule took place. Businesses sending over 5,000 emails daily must have DMARC implemented.

Both companies also have policies for those sending fewer emails. These relate to SPF and DKIM authentication.

Look for email authentication requirements to continue and be more strictly enforced. You need to pay attention to ensure the smooth delivery of your business email.

The benefits of implementing DMARC include:

- Protects your brand reputation
- Improves email deliverability
- Provides valuable insights

*"Email authentication is a way of verifying that your email is legitimate. This includes verifying the server sending the email. It also includes reporting back unauthorized uses of a company domain."*

# Introduction To Smart Home Technology For Small Biz Owners


## Contact Information

**Tech Experts Support Team**
(734) 240-0200
support@MyTechExperts.com

**Main Office**
(734) 457-5000
info@MyTechExperts.com

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

TECH EXPERTS

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




In the past, the concept of a "smart home" might have conjured up images of futuristic living spaces from science fiction movies. Today, technology such as video telephones and voice-activated lights have made those dreams a reality.

However, with the rapid advancement of technology, some traditional problems persist, such as security vulnerabilities and connectivity issues. If you're incorporating smart home technology into your small business, understanding these challenges and knowing how to address them is essential.

Here are some of the most common smart home issues and solutions.

## Connectivity woes

**Problem:** Your smart devices frequently lose connection or have slow performance.

**Solution:** Start by restarting your router and any problematic devices. This often resolves temporary connectivity issues. If problems persist, check the placement of your router. It should be in a central location to evenly distribute the Wi-Fi signal throughout your premises.

For larger spaces, consider investing in a Wi-Fi extender to boost signal strength and expand coverage.

## Device unresponsiveness

**Problem:** Devices fail to respond to commands or operate sluggishly.

**Solution:** The first step in troubleshooting unresponsive devices is to turn them off and on again. This can clear out any temporary glitches affecting performance.

Additionally, ensure your devices are running the latest software updates, as these can include important fixes and improvements.

## Battery drain

**Problem:** Smart devices are consuming battery power more quickly than expected.

**Solution:** Adjust the device settings to optimize power usage. Disable unnecessary features and reduce the frequency of updates or checks that the device conducts autonomously. These small adjustments can significantly extend battery life.

## Incompatibility issues

**Problem:** Smart devices don't communicate or work well together.

**Solution:** Ensure all devices are compatible with your chosen smart home platform (such as Google Home, Amazon Alexa, or Apple HomeKit). When purchasing new devices, review the manufacturer's specifications to ensure they can integrate smoothly with your existing setup. This can prevent a lot of frustration and ensure that your devices can work together seamlessly.

## Security concerns

**Problem:** Vulnerability to hacking and unauthorized access.

**Solution:** Secure all devices with strong, unique passwords. Avoid using default or easily guessed passwords. Implement two-factor authentication (2FA) wherever possible, adding an extra layer of security by requiring a second form of verification to access accounts.

## App troubles

**Problem:** Apps controlling the smart devices frequently crash or lose connection.

**Solution:** If your app isn't working correctly, first try logging out and logging back in. This can refresh the app's connection to your devices. If this doesn't solve the problem, uninstalling and then reinstalling the app may resolve underlying issues.

## Automation gone wrong

**Problem:** Automated functions don't operate as expected.

**Solution:** Review the automation rules you've set up and test them one at a time. This approach helps identify where things are going wrong so you can make necessary adjustments.

## Limited range

**Problem:** Devices far from the Wi-Fi router or hub have poor connectivity.

**Solution:** Move devices closer to your router or smart home hub. This can enhance their communication reliability and speed.

## Ghost activity

**Problem:** Devices activate unexpectedly or exhibit unexplained behavior.

**Solution:** Investigate any unusual activity thoroughly as it could indicate security issues. Change your passwords regularly and monitor device logs for any unauthorized access.

## Feeling overwhelmed

**Problem:** The complexity of managing a smart home system can be daunting.

**Solution:** Take advantage of device manuals and online tutorials. These resources can provide valuable guidance on setup and troubleshooting. If needed, don't hesitate to seek out professional help to ensure your smart home setup meets your business needs efficiently.

By understanding these common issues and solutions, you can better manage smart home technology both at home and in your business, ensuring a smoother, more secure operation. If we can help, please reach out - (734) 457-5000, or info@mytechexperts.com.