Microsoft 365

Security matters:

six tips for small and medium-sized businesses

Introduction

No matter how big your company is, security is a critical part of business. Seventy-four percent of owners of small and medium-sized businesses don’t think they’re at risk of a cyberattack.[1] The truth is that 43 percent of cyberattacks are aimed at small and medium-sized businesses.[2]

If you own a small or medium-sized business, you may feel like you don’t have the time, personnel, or resources to put security measures in place. That’s OK—there are solutions available to help businesses of any size take simple steps to be more secure.

> “When you’re a small team trying to do big things, it can be really tough to try to tackle something that feels like a problem but that might never happen. It’s just human nature to put those things off, and I would say more people don’t prioritize it until they absolutely have to, especially small businesses and early-stage startups sprinting to go to market.”
>
> **Taylor Coil,**
> Marketing Director,
> Tortuga

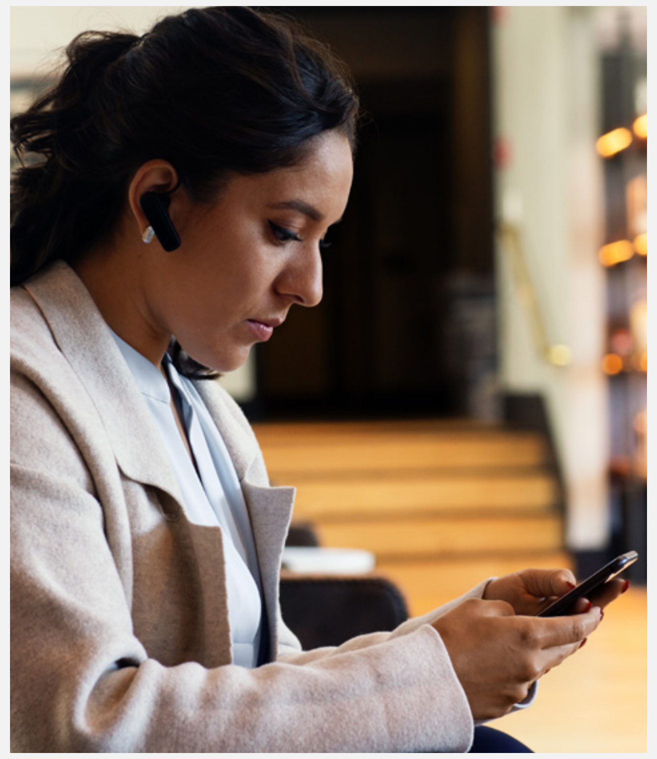
[1] Microsoft’s Global Security Survey for Small and Medium-Sized Businesses.

[2] “Cybersecurity Statistics: Numbers Small Businesses Need to Know.” Small Business Trends, January 2017.

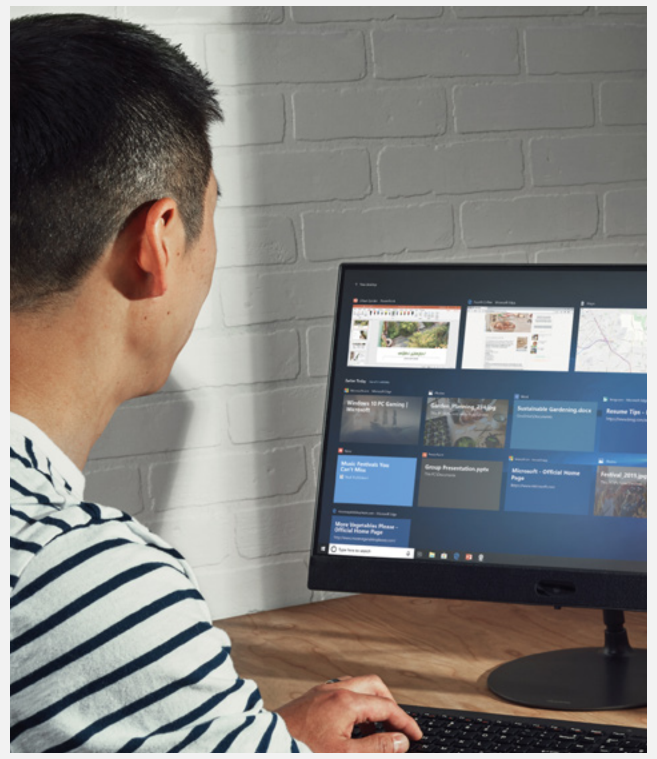
Here are six ways that real small and medium-sized businesses are handling their security.

Treat security as an investment

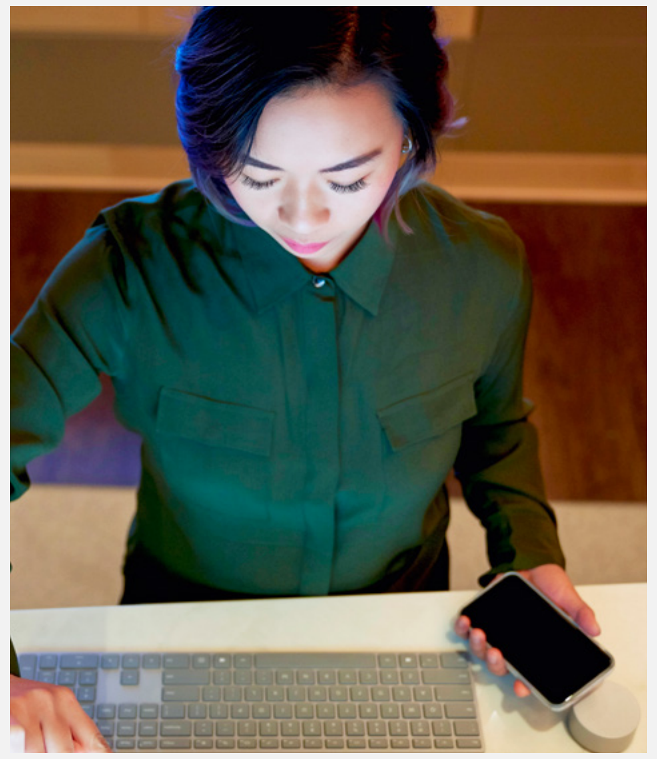
Have an incident response plan



Use technology that helps you manage devices across a diverse and growing mobile environment



Stay compliant with regional security regulations



Take a proactive approach against phishing and other threats

Add security and simplicity for system access

Treat security as an investment

It’s easier to implement security measures early in the process of building your company, rather than trying to apply new security behaviors or practices retroactively.

“Like putting a lock on your front door, it’s very important to protect the assets of your business,” Coil says. That’s especially true for customer data. “We’re the most diligent about securing our [web e-commerce] logins, as well as our analytics platforms, because that’s where most of our customer data lives.”

Andy Freeborn, co-owner of Amethyst Homes, sees security as just another investment in the business, something that customers will notice. “There’s something in that customer interpretation, ‘Oh, they’re running their website SSL secure. It’s probably safe for me to go ahead and make this purchase.’”

This helps customers develop more trust in the company, which can lead to earning more business.

“If customers are trusting us with helping them purchase a sofa or rug, and we’re physically coming into their home, they’re trusting us with that very intimate part of their lives,” says Andy. “Customers also want to know that our website and POS [point of sale] is secure, that they can give their credit card information and not feel like they’re going to be compromised.”

Being associated with lost or hacked credit card information could damage customer relationships.

“Something like that would have a huge impact on us,” Andy says. “Then there’s no trust for future sales, or even conversations.”

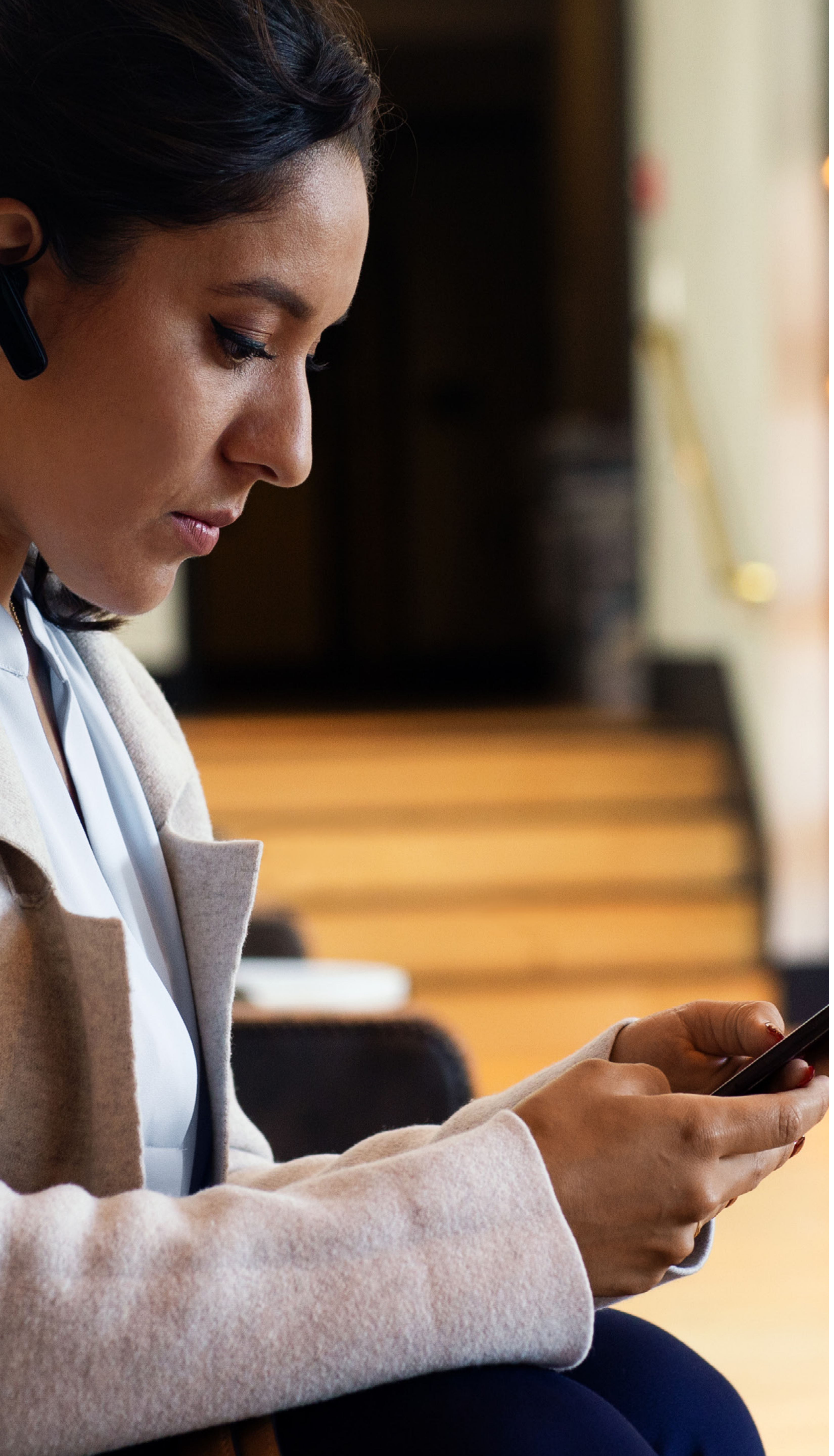
Have an incident response plan

Create a plan for cyberattacks so you know what to do when one happens. Keep Domain Name Server (DNS) records to prevent hackers from spoofing your domain, and reference sites that track compromised credential breaches.

"I've definitely heard of smaller businesses who have received a phishing email, clicked on a link, and now they've got ransomware and have to pay a hefty ransom to get their data back," says Rafael Saucedo, IT manager at regional construction management firm McCown Gordon.

Even with security defenses and a plan, a recent phishing attack was successful at McCown Gordon, but the IT team was able to limit the damage because they had planned for this possibility. IT notified the company of emergency maintenance and shut down the servers. Saucedo analyzed the attack, located and isolated the infected laptop, and began the process of rebooting servers and checking and restoring files. Saucedo's team had backups in place, so only about a day's worth of work was lost.

> I've definitely heard of smaller businesses who have received a phishing email, clicked on a link, and now they've got ransomware and have to pay a hefty ransom to get their data back."
>
> **Rafael Saucedo,**
> IT Manager,
> McCown Gordon



Use technology that helps you manage devices across a diverse and growing mobile environment

Many organizations are not focused on technology because it's not a big part of their core business, especially when it comes to thinking about security from a communications and collaboration perspective. In the absence of clear direction from company leadership, solutions tend to organically emerge without consideration for the inherent security risks.

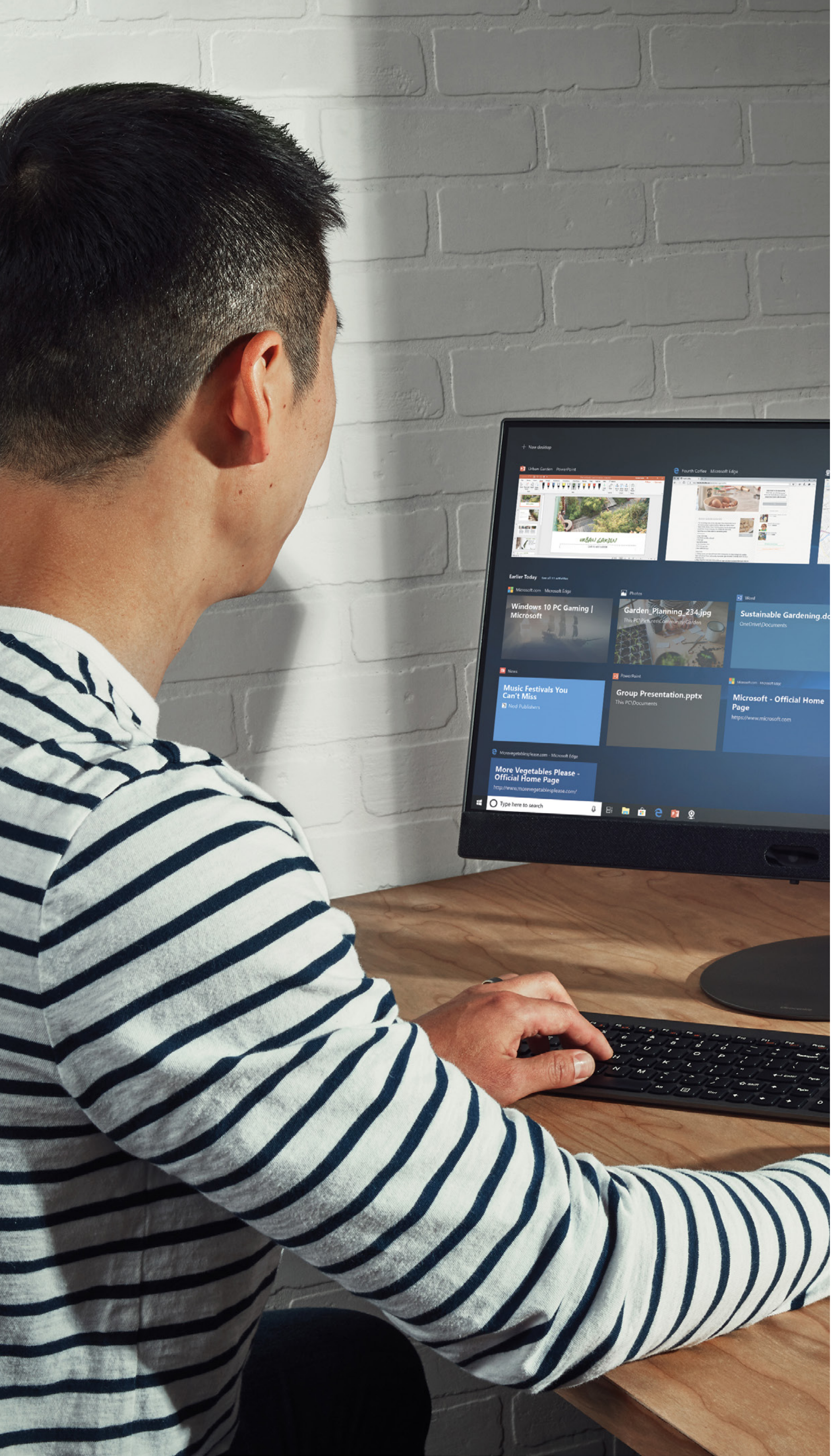
Take professional sports, for example. "It is clear that every employee in every business faces some degree of risk," says Bill Predmore, owner and president of Reign FC, one of nine clubs in the National Women's Soccer League (NWSL) and a two-time winner of the NWSL championship. "[However,] we have a group of employees that have a higher profile than those in the average business."

Prior to adopting Microsoft 365 for business, Reign FC soccer players like Megan Rapinoe, Rumi Utsugi, and Celia Jiménez Delgado mostly worked off their own laptops, tablets, and phones. After one of its star players had her personal accounts hacked, Predmore decided that Reign FC needed a better solution for device management. To help secure devices and store company data, Predmore implemented Microsoft 365. Microsoft 365 for business provides an integrated productivity, security, and device management solution that can help organizations to get up and running.

"For all practical purposes, we've gone from having no meaningful security strategy—nor any security infrastructure in place—to a situation now where we've largely resolved those challenges," says Predmore. "I feel very good about our systems and data being protected."

> The management console makes it super easy to add or take people out at the appropriate time. It has cut the burden of administration down significantly, and at the same time massively increased the sophistication of the technical infrastructure.”

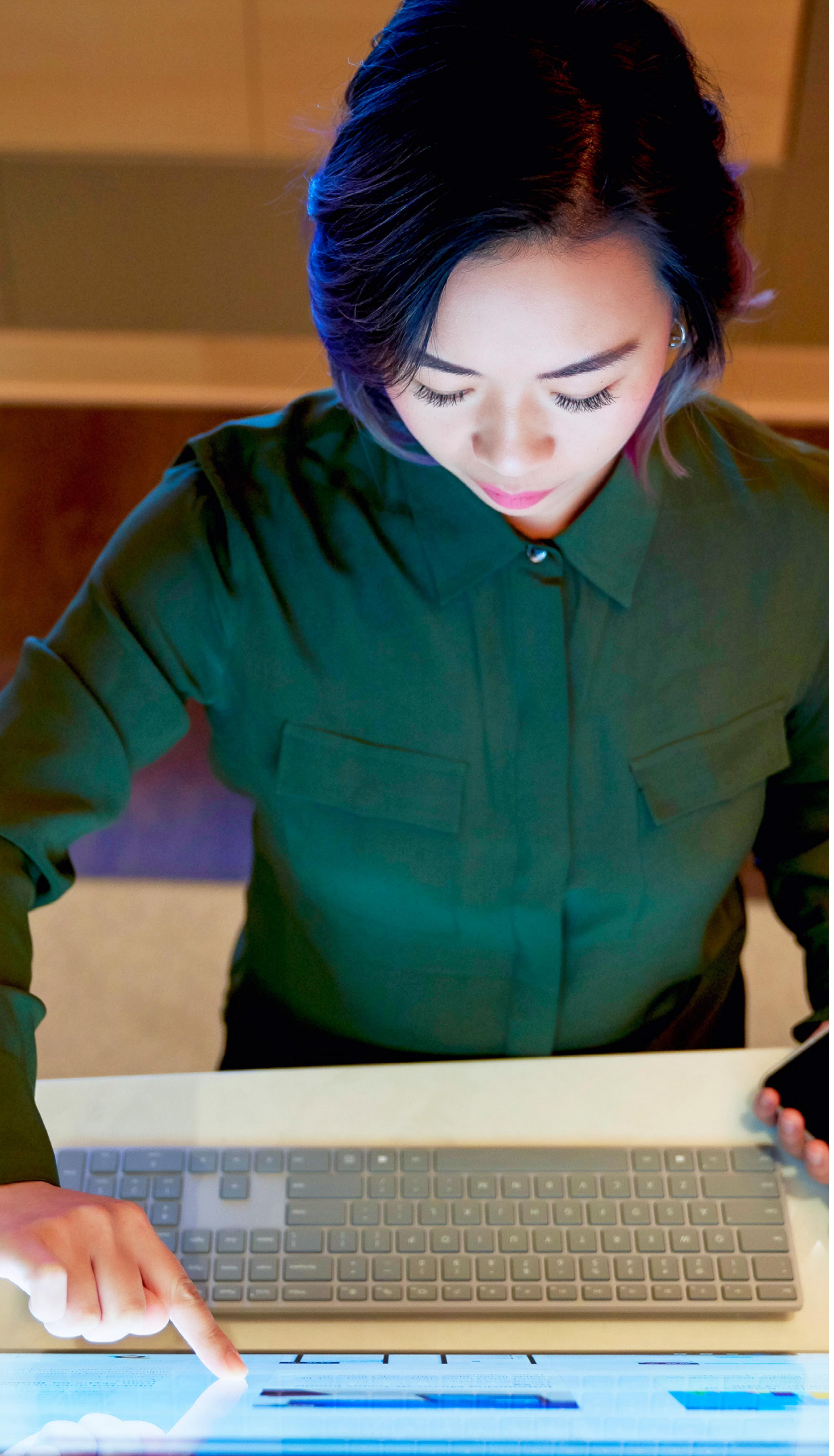
Bill Predmore,
Owner and President,
Reign FC, Predmore.



Stay compliant with regional security regulations

For businesses that work with customers in the European Union (EU), compliance with the General Data Protection Regulation (GDPR) must be a security consideration. Handling any data from EU residents requires careful attention to personal privacy rights, data protection responsibilities, and breach reporting guidelines, at the penalty of significant fines.

For GDPR compliance out-of-the-box, Microsoft 365 has you covered. Microsoft is GDPR-compliant across our cloud services, and we manage our own GDPR compliance as both a data controller and a data processor. We provide the contractual guarantees you need under the GDPR, and we continue to build features and capabilities into our products and services.



Take a proactive approach against phishing and other threats

Small actions every day can help people do their jobs more securely.

"It can be a series of low-effort tasks in the beginning," says Saucedo, "but that can have a lasting impact."

About once a month, McCown Gordon provides training on how to detect phishing emails by checking the sender's email address and domain, and hovering over links to see the actual URL.

Protecting against phishing is critical for small and medium-sized business owners—between 90 and 98 percent of all cyberattacks begin with phishing.[3] Today's phishing attempts are better camouflaged, propagate rapidly, and can even evolve to evade detection.

Even trickier are spear-phishing attacks, where the email is highly targeted to the person receiving it, like someone in accounting getting an email sent from someone posing as the CEO requesting a wire transfer. Because even a cautious employee can be fooled by a sophisticated phishing attack, it also helps to invest in tools such as Microsoft 365 for business that automatically scan and filter emails and attachments for threats.

Microsoft 365 is built on top of the Intelligent Security Graph, which updates all Microsoft platforms and services around the world whenever a new cybersecurity threat is detected.

[3] "Defend against threats," Microsoft. 2020.

Add security and simplicity for system access

Enable multifactor authentication for layered security. Two-factor or multifactor authentication requires two or more secure elements to access an account—like a code sent via email or a biometric or fingerprint scan.

In addition to using two-factor authentication, Tortuga requires employees to use a password manager to help them generate and manage unique, random passwords.

Coil explains, “If we were to get hacked because I’m logging in to [our e-commerce platform] from an airport or from a coffee shop in Berlin, then that one hacked website doesn’t lead to a hacker having access to all of our accounts. And if we are on one of those lower security networks, then we use a VPN,” or Virtual Private Network, an encrypted connection to another network over the Internet.

McCown Gordon also requires unique usernames and passwords. Saucedo says, “The big shift for us has been empowering our remote workforce through cloud solutions. With so many different cloud providers and identities to manage, we utilize Microsoft’s Active Directory Federation Services (ADFS) for single sign-on,” or SSO.

“SSO is a big help, enabling employees to sign in once to access multiple resources,” says Saucedo. “Thus, they only have to keep track of one username and password.”

Serious security can start with small steps

More than 70 percent of businesses report feeling vulnerable to a cyberattack, often because they lack the knowledge, resources, and expertise of larger organizations.[4] Modern technologies such as Microsoft 365 can make security simpler and easier for small and medium-sized businesses, with comprehensive protection, built-in safeguards, and easy-to-use tools.

[4] "Small Business Cyber Security Study," Microsoft & YouGov, April 2018.

Working in a growing business is exciting and rewarding. A thoughtful, deliberate approach to security can make your daily challenges and accomplishments even more satisfying, by giving you the confidence and peace of mind that you're protecting what you've built.

Have more questions? Contact us. Or learn more about Microsoft solutions for your business.

Microsoft 365