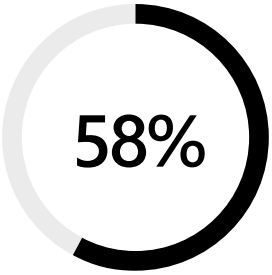
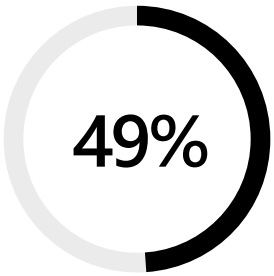
The 10 don’ts of small business security

Microsoft

For the most part, we only hear about security breaches when they happen to celebrities, or attacks that target large multi-national companies. But the reality is that small and medium-sized businesses are just as much at risk. How much is your customer, transactional, and operational data worth to you?



of breaches target smaller businesses.



involve malware.

Verizon 2018 Data Breach Investigation Report

Beef up your digital security by understanding what not to do. Here are 10 security don'ts to protect and defend your organization.

01

Don’t click first and ask questions later

Cyber criminals are getting craftier. They may use bots to write and deploy phishing scams. It can be tough to differentiate fake from genuine communications. Be mindful and look for the signs. Train yourself and your staff to be cautious and to avoid:

- Opening unknown attachments
- Responding to random requests for info
- Clicking on suspicious links

54%

of small businesses have had breaches involving customer and employee information in the last 12 months.

Ponemon’s 2017 State of Cybersecurity in Small & Medium-Sized Businesses

59%
of small business lack visibility into employee password practices, like using weak passwords or sharing them.

Ponemon's 2017 State of Cybersecurity in Small & Medium-Sized Businesses

02

02

Don't use dumb passwords

Just because it still works doesn't mean it's safe. In fact, relying on an old device or outdated software can put you at risk. Your IT team has better things to do than run virus software checks or retrieve lost files.

If your business is still running Windows 7 or an old version of Office, you're leaving your business vulnerable. Upgrade to Windows 10 and Office 365 that have built-in security features.

03

Don’t rely on out-of-date technology

Just because it still works doesn’t mean it’s safe. In fact, relying on an old device or outdated software can put you at risk. Your IT team has better things to do than run virus software checks or retrieve lost files.

If your business is still running Windows 7 or an old version of Office, you’re leaving your business vulnerable. Upgrade to Windows 10 and Office 365 that have built-in security features.

Replace those old machines! Old PCs experience problems nearly twice as often as newer ones.

Techaisle’s SMB PC Study, 2018

04

Don’t ignore your devices

If you’ve equipped your teams with mobile devices, great. Just don’t forget their personal ones that they use while on the job. Password-protect every phone, tablet, and laptop. Then, increase security by leveraging Microsoft’s built-in Mobile Device Management for Office 365 to allow you to lock, wipe, and reset a lost or stolen device remotely.

05

Don’t go it alone

Leverage the huge investment Microsoft makes in security. Store, secure, and unify your data safely behind firewalls in our cloud. SharePoint makes file sharing lightning-fast and keeps your team from using thumb drives and other devices that can get lost or stolen. Use OneDrive, Office 365’s cloud storage service, to automatically back up your files and restrict access to documents and files for another layer of protection for your data.

06

Don’t overlook encryption

Many emails contain sensitive data and it’s easy to encrypt sensitive emails using Outlook and Office 365. Looking for a one-click solution? OneDrive for business can password-protect files saved to the cloud.

07

Don’t assume your apps are safe

Backing up your files is one issue, but your apps are just as important. Many small businesses rely on inventory systems and accounting software to function every day. For mission critical applications, we recommend hosting and optimizing apps using Azure services like the Microsoft Cloud Toolkit for Business.

08

Don’t forget fixes and updates

Windows 10 and Office 365 may update themselves automatically, but what about the other software you use? Don’t trust outdated apps, operating systems, or browsers. Ignoring updates puts your business at risk.

09

Don’t just plan for the best

Even small business owners should invest the time and resources to develop a disaster recovery strategy, which ensures your business continuity, come what may. Luckily, Azure Site Recovery service automates the process for businesses. By leveraging Microsoft’s global network of datacenters to create redundancy, Azure can ensure your business has secure and uninterrupted access to your applications and data. Period.

The Microsoft Cloud spans more than 100 highly secure facilities worldwide—all linked by one of the largest networks on Earth—and monitored 24/7/365.

Microsoft

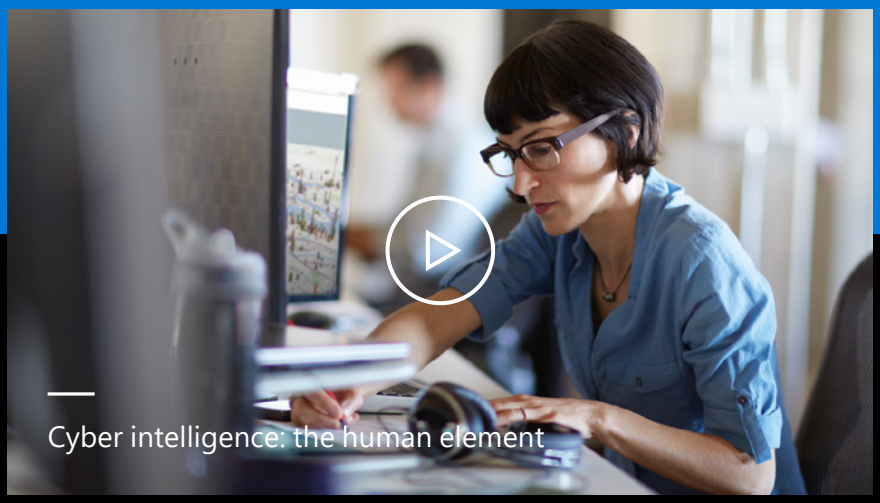
10

Don’t just talk about it

It’s going to take more than a single email to train your employees to understand the risks and recognize the signs of scams and potential breaches. Explain why it’s important and what can happen if a security breach occurs. Your team has a vested interest in your business’ success. Make security part of your corporate culture.

Watch the webinar

Discover how to motivate your team to help prevent a security breach. This video from the Modern Workplace series focuses on the human element and what you and your team can do.



Get expert help

Already working with a Microsoft partner? Ask them how you can improve your digital security. If you aren't working with a partner, let us introduce you to some in your community. Visit the Microsoft Solution Providers page to find one near you.