



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Canner, Ben

Title: "How Small Businesses Can Stay Safe Online"

Website: cpomagazine.com

Organization: CPO Magazine

Date: 06 April 2019

URL: <https://www.cpomagazine.com/cyber-security/how-small-businesses-can-stay-safe-online/>

Accessed: 09 July 2019

Synopsis: For modern businesses, the internet is a crucial commercial tool, and one you'll utilize each and every day. The ability to email, work remotely and operate a website will be imperative to the everyday operation and ongoing success of your venture, but it only really works if you're able to do everything you need to safely.

At their heart, the basic security rules for commercial enterprises are not so dissimilar to those you'll apply to your personal computers and communication devices, but the difficulty lies in not only ensuring that you're doing everything you need to, but that everybody else who's involved in your operation is on-board too.

So how exactly can you safeguard the security of your small business? What do you and your employees need to know? Here are a few tips you might find useful.

Know what to expect
from the CCPA



[View the infographic](#)

MICRO
FOCUS

[Home](#) > [Cyber Security](#) >



CYBER SECURITY INSIGHTS

How Small Businesses Can Stay Safe Online



Matt Powell

On **Apr 6, 2019**

[f](#) Share [t](#) Tweet [in](#) Share [p](#) Pin it [+](#)

For modern businesses, the internet is a crucial commercial tool, and one you'll utilize each and every day. The ability to email, work remotely and operate a website will be imperative to the everyday operation and ongoing success of your venture, but it only really works if you're able to do everything you need to safely.

- Advertisement -

At their heart, the basic security rules for commercial enterprises are not so dissimilar to those you'll apply to your personal computers and communication devices, but the difficulty lies in not only ensuring that you're doing everything you need to, but that everybody else who's involved in your operation is on-board too.

So how exactly can you safeguard the security of your small business? What do you and your employees need to know? Here are a few tips you might find useful.



Reinforce the importance of keeping software and operating systems up to date

Most of us have been guilty of it: seeing a notification pop up onscreen and clicking off it with barely a glance at the information it contains. A lot of the time, these little text boxes are telling us that a security update for our operating system or software has become available, and while you might already be paying attention, it's time to make sure your employees are doing the same. Any time that you're able, try to reinforce the importance of downloading and installing the tools at their disposal to your workers so that everyone's tech has access to the most up-to-date and efficient protections out there. Fail to do this, and you might find that while you're doing your part, the laxity of others means your company is not so well protected from emerging threats as you previously supposed.

Before you continue reading, how about a follow on LinkedIn?

 Follow

Secure your wireless networks

Those individuals who are not technologically savvy may lack an understanding of what an open network even is, but all they really need to know is that these act as an invitation for anyone out there to connect to your IT network and compromise it.

The best way to address this is, of course, simple: you secure your wireless networks with strong passwords that the average person has no hope of guessing. These should naturally include both numbers and letters, but that can mean they're difficult to remember. As a result, you might find your less-informed employees have a habit of noting them down in plain sight – something you need to vehemently discourage. Just in case anyone fails to get this memo, we also recommend that you enforce regular password changes. This means that even if someone does stumble across some hastily annotated information, it will do them little good once the password alters.

Set up firewalls

There are dozens of different ways for savvy SMEs to stay safe, and one of the easiest and most efficient is to set up firewalls. Firewalls work by protecting your internal networks from threats, which is why we recommend installing them not only on your servers, but on all office laptops, computers, and mobile devices too. These should make a real difference to your security, but in order to make sure they're operating to the best of their ability, you will need to be proactive and keep them up to date – a memo that must be passed on to your employees. If they don't know how to stay safe, they can't be held responsible for any weak points they inadvertently create.

Secure access to your devices and computers

When it comes to maintaining a secure workplace, it's not enough to simply do one of these things and hope for the best. You need to have a cohesive strategy in place that covers every eventuality. This means that on a more physical level, you should also be doing your utmost to keep unauthorized visitors out of your office space, and to make sure that any easy-to-grab devices – such as laptops or mobiles – are stored securely and outfitted with remote tracking software. If you want to go the whole hog, we suggest that all portable tech is encrypted too, from laptops to USBs and DVDs. Not only is this easy to do, but it can significantly reduce the cybersecurity risks attached to lost or stolen office equipment.

Educate your employees on cyber safety

No matter how sophisticated your security software is, its users need to know how to take advantage in order for it to be truly effective – that means educating your employees. It's no good having all of this technology at your disposal if those who work for you are going to put your business at risk by clicking on infected pop-ups or falling for phishing scams. So how best to combat this issue? The answer lies in proper training, whether this is delivered by you or by specialists who have a greater understanding of how cybersecurity works. Teach your employees the safest way to use the internet, and you'll be doing a huge service to your company as a whole.

Educate yourself

It's not only your employees who need proper training. The same applies to you, so you might want to see what courses are out there to help broaden your understanding of the issues you're facing. If you don't want to splash out on such a service, there are plenty of other ways to educate yourself, and the internet is a wonderful resource. If you're using your computers for more than just business (which many of us do in our lunch hour or on an evening) make sure that it's not only professional security protocols you look into, but personal ones too. For example, if your poison is online gambling, know how to vet online providers by using sites such as Oddschecker, which vows to only feature fully licensed bookies, that are secure and trusted. Similarly, if your weakness is online shopping, resources like Trustpilot will help reassure you that you're buying from reputable retailers.

Install anti-virus solutions

Although some small businesses don't like to limit what employees are able to view online – as their equipment will often be for both personal and professional use – considering a restriction on access to inappropriate websites is a veritable alternative that can reduce the risk of exposure to malware. Whether you choose to do this or not, malware is a threat you need to take seriously. We suggest installing anti-virus solutions on all of your systems. This, of course, will work best when kept up to date, so we recommend implementing a policy with regards to when and how security updates are installed. The more frequently you do this, the better protected you will be – a point worth bearing in mind.

When it comes to keeping your workplace safe from cyber threats, it pays to be prepared, and the more proactive you are, the less likely you'll be to find yourself dealing with the unpleasant consequences of falling victim to online crime. Follow our top tips and tricks, check out the handy resources listed here, and you should find that your business is just fine.

[f Share](#) [t Tweet](#) [in Share](#) [p Pin it](#) [+](#)

- Advertisement -

Free Active Directory Tool

Track lo
change
tool. Ge
Now!



Matt Powell

Staff Writer at CPO Magazine

Matt is a researcher and writer. He has previously worked for large multinational companies in the areas of content marketing and public relations.