Internet security and COVID-19 scams

Cybercrime has advanced along with technology. It doesn't matter if you have 1 or 100 computers connected to the Internet – understanding the threats posed by cybercrime and training staff to spot them is a must for doing business.

Beware of Covid-19 scams

Every crisis brings out the worst in people and COVID-19 is no different. There are a number of scams targeting individuals and small businesses.

Watch out for:

- Emails claiming to be from the Government or the World Health Organization asking for personal or financial information
- COVID-19 related investment scams
- Miracle products claiming to prevent, detect, or cure COVID-19
- Online retail fraud and counterfeit goods related to the virus
- Donation or fundraising scams
- Red Cross/charities offering free medical products (e.g. masks) for a donation
- Private companies offering fake COVID-19 tests for sale
- Emails pretending to be from us asking for financial details

Fake text messages

Coronavirus-themed SMSs are also delivering malicious software to smartphones. The text messages look like legitimate organizations and request you to click on links or open attachments.

This software is typically designed to steal banking credentials.

Spotting suspicious messages

There are usually a few red flags that can help you spot a suspicious message. These tell-tale signs of a suspicious message include:

- Not from a known email address
- No personalized greeting
- Unfamiliar phrases and poor language
- Written with a sense of urgency
- No return contact details provided
- Embedded links
- Old/incorrect branding.

The scale of cybercrime

Cybercrime covers many illegal and unscrupulous activities on the Internet. These include identity theft, fraud, and spreading computer viruses or malicious software known as 'malware.'

Cybercriminals are increasingly focusing on mobile devices such as tablets and smartphones, and on social networks like Twitter and Facebook.

Two-thirds of adults have already been victims of cybercrime in their lifetime. You probably think it won't happen to you but small businesses often have less sophisticated IT security measures than larger organizations, making you an easy target.

Understanding the threats and developing an Internet policy for employees are both essential to defending your business against cyber attacks.

What are the most popular targets?

Common threats include malware and data theft – below we outline what cybercriminals are aiming to achieve in these instances.

Data theft

The aim of cyber criminals here is to:

- Find out your company's credit card details.
- Obtain your online banking access details to steal from your account.
- Access your customer databases – these are either sold on to other criminals or used directly to commit identity theft and fraud.

Espionage and malware

Industrial espionage and attempts to steal your intellectual property (IP) are also on the rise. These crimes are often achieved through malware, or malicious software usually downloaded without the user's knowledge as an attachment to programs and even bogus antivirus software.

Most malware bugs transmit data over the Internet, including your browsing habits and other personal information. More dangerous forms of malware include keylogging software that records what you type on other websites, such as online banking and email passwords.

How to reduce the risks

Reduce your exposure to these risks by:

- Limiting staff access to commercially valuable information on a need-to-know basis.
- Requiring employees not to download any programs without permission.
- Making your staff aware of the risks of IP theft and espionage to prevent them unknowingly providing sensitive information.

Protect your business's weak points

Cybercriminals will always attack the weak points in your Internet security first.

To combat this:

- Make sure firewalls are turned on and your antivirus program is up to date.
- Require staff to review any passwords they use to access their workstations. It's easy to become lazy about passwords and this can offer an open door for criminals.
- Ensure passwords are long (typically 7-10 characters), contain both upper and lowercase letters, along with numbers. Ensure they aren't similar to other passwords staff use to access personal sites, like Facebook or online banking websites.
- Make a point of changing passwords regularly.
- Install a server-based spam filter to reduce spam reaching your business's inbox.

Mobile devices

Two-thirds of people don't have any security solution on their portable devices, so apply all of these practices to mobile work devices with Internet access, such as smartphones and tablets.

Security training should be a necessity

It's hard to control employees using the Internet at work to access personal emails or their social media accounts. But it's important to develop some rules around the use of work computers. You need to control both wasted working time and staff infecting business computers through careless behavior.

Being aware of viruses

Many viruses are spread as email attachments that appear to be harmless. An email will often encourage the reader to open an attachment by pretending to be a joke, video clip, photograph, or some breaking news.

Train staff to avoid:

- Using their work email accounts for personal messaging.
- Opening attachments or clicking on links in emails from friends, colleagues, or unknown people. Infected files can be forwarded to contacts without the sender being aware.
- Using file-sharing networks at work to download movies, videos, or music.
- Being deceived by fake messages or fake websites (known as phishing) that try to manipulate the user into revealing sensitive information such as account details or passwords.

Impress upon staff that Internet security is also critical to maintaining the confidence of customers. Compromising customer details or sensitive communications could cost the business both credibility and customers.

When working remotely

Internet security doesn’t end with work computers. Working from home or using mobile broadband or Wi-Fi hotspots also exposes your business to potential threats. Make sure every device connected to the Internet has the latest software updates and antivirus protection.

Deploying a policy

Your policy should clearly state who’s responsible for implementing the plan and carrying out ongoing monitoring.

If your business has more than a few employees or uses a departmental structure, include a timetable for security implementation so everyone stays on the same page – communication is the key.

Seek advice

Training your staff to avoid the pitfalls of inappropriate Internet use can be as simple as developing a company Internet policy with guidelines for safe practice. The benefits of this type of training include a reduction in the risk of security issues arising and improved IT, and online skills in your staff.

- Conduct an internet security audit to see how protected you and your staff are
- Allocate a person in the business to be responsible for security updates
- Add internet security into employee agreements so they know the severity of non-compliance.

If you found this article useful, visit voyage.harborone.com for business advice, tools and templates. Topics include business recovery, improving cash flow, growing sales and succession. Plus access free business plan and cash flow templates, calculators and checklists.

Disclaimer

For informational purposes only. There is NO WARRANTY, expressed or implied, for the accuracy of this information or its applicability to your financial situation. Please consult your financial and/or tax advisor.