Guide
Securing your company against online threats

Close Brothers
Invoice Finance

Securing your company against online threats

Online capabilities have advanced greatly during the last decade. You can send money across the world in less than a minute, simultaneously work on documents as a team and even have a real time conference call with businesses in all four corners of the globe. All you need is a device with an internet connection.

But with the positive comes the negative as private information, finances and sensitive documents have never been more at risk from online threats and criminals who actively attempt to access information for unlawful gain.

You may have seen press reports on the *Heartbleed*[1] or *Gameoverzeus*[2] computer viruses (otherwise known as "malware") which have already infected over 15,000 computers in the UK and many more worldwide. Computer viruses and cybercrime are becoming a major threat for businesses of all sizes.

Current figures estimate that the annual cost of "cybercrime" to the global economy is over $400 billion dollars (£238 billion)[3]. This activity typically takes the form of computer viruses that infect hardware and enable a hacker to access the computer to either take control of it, lock it for cash payment, or at the very worst, silently gather details to enable them to access bank accounts and other financial information at will.

Fortunately there are some very simple steps that can be taken to protect businesses from cybercrime. This guide will offer you a basic overview of what areas of your business you need to secure and protect from cyber attacks.

Email security

Emails are now a way of life for every business, whatever the size. This also means that spam mail (the email equivalent of unsolicited junk mail) is a problem for anyone with an email address. Email is the primary platform that viruses use to spread and get into your computer, in the form of an attachment or a message that requests the recipient to click on a website link. The way to protect yourself against these threats is simple; if you don't recognise it, don't click on it.

Below are the typical signs that an unsolicited email poses a threat:

- The title has "re:" in it to give the impression it's replying to a message you sent (for example: "re: hello"). If you didn't send a message with that title, don't open it.
- The email refers to a parcel waiting for collection and encourages you to open an attachment or click on a link to learn more. If you don't recognise the retailer or are suspicious about the content (e.g. unidentified email address, spelling mistakes or poor grammar), do not click any links in the email and either delete it, or forward it to an IT professional who can block any further communications from this address.
- Any attachment from an unknown source or sender should be treated with caution. The primary attachments used to infect computers end in ".zip" or ".exe".

There are still likely to be cases where employees unwittingly open an infected attachment or link, so it is important that your staff are educated on the dangers of cybercrime and how to avoid it. Getting a firewall installed to protect your server will immediately negate the majority of threats contained in emails. In all cases, any emails thought to contain a threat should be deleted or sent to your IT professional.

Anti-virus

The most powerful tool against online threats is anti-virus software that can protect computers and servers against attack. This software recognises and protects your computer against most known malware. It is equally important to keep your anti-virus software up-to-date to ensure protection against the latest threats. You can obtain fairly basic free software online, but a for-fee product will offer a far greater level of protection which will be worth the cost.

> "The way to protect yourself against these email threats is simple; if you don't recognise it, don't click on it."

Protecting data

Data is a fundamental part of any business. The way you protect this needs careful consideration. For example, you might go to work one day to find your servers have been infected with malware and that all of the files and information you keep are irrecoverably lost. Further to this, it is a legal obligation to protect this information under the 1998 Data Protection Act.

You need to ensure that your data is backed up on a daily basis – that way, in the event of an infection you won't lose all of your data. An alternative is to securely store it in the "cloud" (a topic covered in our last guide, available on our website).

Maintenance

Whatever the size of the company, it is advisable that at least one IT professional is supporting the security and general upkeep of your IT infrastructure.

While the points mentioned above go a long way in protecting you from online threats, it is still vital that you maintain all company computers:

- Ensure your staff have the correct hardware (laptops, printers etc.) and tools to carry out their responsibilities.
- Keep your operating system (OS) and application software up-to-date to make sure any new software you want to install will be compatible.
- Install software updates when prompted so that hackers can't take advantage of known problems or vulnerabilities.
- Keep OS platforms updated to the current supported versions (for example Microsoft recently stopped supporting the Windows XP OS).
- Make sure that your PC or IT environment has the capacity to support your business requirements.

The majority of these measures can be performed by you, however if some of the above seems overwhelming, don't be alarmed as they can be carried out with ease by an IT professional. This will ultimately safe-guard your business against potentially time consuming and costly threats in the long run.

1 www.techradar.com/news/internet/the-heartbleed-bug-has-made-the-internet-s-secure-websites-very-insecure-1241004
2 www.bbc.co.uk/news/technology-27681236
3 Macafee report June 2014 – "Net Losses: Estimating the cost of cybercrime"

If you're looking for working capital or additional funds to support your business please call Close Brothers Invoice Finance on 0808 149 8672 or visit www.closeinvoice.co.uk

Close Brothers Invoice Finance