

## Cyber Crime – are you really safe?

### BREAKING NEWS

UK 'Losing War Against  
Cyber Crime', warn MPs

30 JULY 2013

**An influential group of MPs has today warned that the UK is losing the war against internet crime.**

**Despite being the preferred target of online criminals in 25 countries, the UK is still "complacent" towards e-crime as victims are "hidden in cyberspace", the Home Affairs Select Committee said. [Press Association 30 July 2013]**

**To back this up, a recent report from The Federation of Small Businesses (FSB), shows that small firms lose £785m a year to cyber criminals and online fraudsters, losing on average £4,000 (€4,732, \$6,099) each from cyber crime, with 41% having fallen victim to prowling online criminals in the past year.**

**Among the FSB's recommendations is the creation of a new national advertising campaign to raise awareness of Action Fraud, a police facility for the reporting of internet fraud and an information hub on how people can protect themselves against hackers and web criminals.**

**Fortunately, there are simple things you can do to take control and help protect yourself and your business. The most important investment you can make is to take the time to identify where you may be at risk from fraud.**

Whilst all businesses are different, there are general principles that can be applied regardless of size or type. There is no one-size fits all approach to fraud prevention. Instead, it is about knowing where you could be at risk and adopting a general mindset of awareness and action in the parts of your business that could be vulnerable.

There are many different kinds of cyber crime. A criminal might try to gain access to your information - like your email password, banking details or National Insurance number. They might do this by installing malware on your computer, trying to hack into your account or tricking you into giving them the information. Then they could steal from you, impersonate you or even sell your details to the highest bidder. Or divulge critical, confidential information about your business to a third party source.

A criminal might also try to use the Internet to scam you, sell you fake goods or make you do things that cost you money. Or, like a thief who steals a getaway car without caring who the owner is, they could want your computer or a website that you own to use as a tool to commit cyber crime (pretending to be you!)

### Secure your passwords

Passwords are the first line of defense against cyber criminals. It's crucial to pick strong passwords that are different for each of your important accounts and it is good practice to update your passwords regularly. Follow these tips to create strong passwords and keep them secure:

- *Use a unique password for each of your important accounts like email and online banking*

Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office - if a criminal gains access to one, all of them are compromised. So don't use the same password for an online newsletter as you do for your email or bank account. It may be less convenient, but picking multiple passwords keeps you safer.

- *Keep your passwords in a secret place that isn't easily visible*

We all know someone who has their password written down on a Post-It note stuck to the front of their computer or in their top right hand drawer. Keeping a record of your password is not necessarily a bad thing, but keep that record secure. There are a number of electronic password keepers that are themselves password protected. You need only remember one password, the access one, and the software will generate secure passwords for you, store them and submit them when you log in.

- *Use a long password made up of numbers, letters and symbols*

The longer your password, the harder it is to guess and therefore the more secure your information is. Adding numbers, symbols and mixed-case letters makes it harder for would-be snoops or others to guess or crack your password. Don't use '123456' or 'password', and avoid using your favourite football team followed by a number 1 to 9. It's not very original and it isn't very safe!

- *Try using a phrase that only you know*

The phrase might be related to a particular website to help you remember it. For your bank, for instance, you could start with "My banks charges are too high" and then use numbers and letters to recreate it; "Mbc2Hi". Then repeat this process for other sites.

- *Set up your password recovery options and keep them up to date*

If you forget your password or get locked out, you need a way to get back into your account. Many services will send an email to you at a recovery email address if you need to reset your password, so make sure that your recovery email address is up to date and still accessible. Better still, register your mobile number with them and they can send a verification code direct to your phone.

## Prevent identity theft

Cyber criminals have many different ways to steal personal information and money. It's important to know the common tricks that criminals employ to help you protect yourself from online fraud and identity theft. The most obvious thing to say is don't reply if you see a suspicious email, instant message or webpage asking for any of the following details:

- Usernames
- Passwords
- National Insurance numbers
- Bank account numbers
- PINs (Personal Identification Numbers)
- Full credit card numbers
- Your mother's maiden name
- Your birthday

Don't fill out any forms or sign-in screens that are linked to those messages. If someone suspicious asks you to fill out a form with your personal information, don't be tempted to do so. Even if you don't hit the "submit" button, you might still be sending your information to identity thieves if you start inputting your data into their forms.

Be savvy about what is 'suspicious'; no one trusts an email from someone they don't know or they believe is unsolicited. But 'suspicious' also includes service providers that you know and are used to dealing with. In just the last month I have received emails purporting to be from:

- PayPal, advising me that there had been a number of failed attempts to access my PayPal account and unless I completed the attached form confirming my details the account would be suspended. PayPal don't use this method of communication regarding accounts, if there was a problem with the account I would be notified the next time I logged in.

***NEVER*** follow a link in an email, even if it is from a service provider you deal with regularly.

***NEVER*** enter your password unless you have gone directly to the site by using a bookmark or typing in the site's address directly into the browser.

- PayPal, purporting to acknowledge a scheduled payment I have set up, always in \$; I am to follow the link if I want to edit or cancel the payment.
- Shutterstock, advising me my VAT number was incorrect, requiring me to log into my account, following the link in the email, to update my details. This was followed by an apology email to say the first was sent in error, please follow the link in the email for further details.
- Incoming fax report, requiring me to log into a website, following the link in the email to view the fax online. No personal information required, but by simply clicking the link I could be downloading Malware/Spyware onto my computer, enabling the cyber criminal to access my personal data and log my passwords.
- LinkedIn connection requests from people I don't know; follow the link to connect to them. Click on their profile and it does not take you to LinkedIn. Following the link could however download Malware onto the computer.
- Docusign email to say 'your document is complete please click on the link in the email to access the document' - when I was not expecting to receive a document.

## Securing your computer and data

- *Keep your browser and operating system up to date*

Most operating systems and software will notify you when it's time to upgrade - don't ignore these messages and update as soon as you can. Old versions of software can sometimes have security problems that criminals can use to more easily get to your data, and this is important for businesses to remember. What's good to know is that Google's Chrome browser automatically updates to the latest version every time you start it up, so that you can get the most up-to-date security protection without any extra work.

- *Only use trusted sources for downloading software*

When you do install software, make sure that you're getting the software from a trusted source. Some programmes bundle Malware as part of their installation process. Check for online reviews or comments about that particular download.

Be wary of pop-up windows that ask you to download software or that offer to fix your computer. Often these pop-ups will claim that your computer has been infected and that their download can fix it - don't believe them. Close the window and make sure you don't click inside it.

- *Don't just buy Anti-Virus software, update it regularly and run it*


Although a reputable anti-virus software will run in the background checking incoming messages and websites, it is still advisable to run the programme across the whole network and keep it updated regularly; viruses and malware are constantly being written and adapted so regular updates are imperative, both at home and at work.

If you notice something suspicious after a download - such as significant computer slowness, unexpected pop-ups or messages, or unfamiliar billing charges - uninstall the software immediately and make sure your anti-virus is running and up to date.

Consider restricting which employees can download software within your business.

- *Use secure networks*

It's good to be extra careful whenever you go online using a network that you don't know or trust - like using the free Wi-Fi at your local cafe. The service provider can monitor all traffic on their network, which could include your personal information. In addition, when you connect through a public Wi-Fi network, anyone in the vicinity can monitor the information passing between your computer and the Wi-Fi hotspot if your connection is not encrypted.

Check for signals that your connection is encrypted. Look at the address bar in your browser to see if the URL looks real. You should also check to see if the web address begins with `https://` - which signals that your connection to the website is encrypted and more resistant to snooping or tampering. Some browsers also include a padlock  `https://www.google.co.uk/` icon in the address bar beside `https://` to indicate more clearly that your connection is encrypted and that you are more securely connected. To be even safer avoid doing important activities like banking or shopping over public networks.

If you use Wi-Fi at home, you should make sure that you use a password to secure your router. Just follow the instructions provided by your Internet Service Provider or router manufacturer to set your own password for the router instead of using the router default password, which may be known to criminals. If criminals are able to access your router, they can change your settings and monitor your online activity.

Finally, for an added layer of security, you should also make sure to secure your home Wi-Fi network so that other people can't use it. This means setting up a password to protect your Wi-Fi network - and just like with other passwords that you choose, make sure you pick a long, unique mix of numbers, letters and symbols so that others can't easily guess your password. You should choose the WPA2 setting when you configure your network for more advanced protection.

This should be mandatory for all employees that work from home, even on an occasional basis, where they are able to access the company's network.

- *Take regular backups and implement a Business Continuity Plan*

One of the most frustrating experiences that a business can go through is to see files lost or damaged by a computer virus. Hackers are continuously creating new virus threats and it's important to protect your files and computer hardware by having virus protection in place. In addition to maintaining your anti-virus software, make sure you take regular back ups and have a plan ready should the worst befall you. Only by planning to deal with the loss or corruption of data can you minimise the damage to the business.

To read more about Protecting your Business Against External Fraud, visit our website at [http://www.aquilaadvisory.co.uk/articles\\_and\\_publications.html](http://www.aquilaadvisory.co.uk/articles_and_publications.html)

## Aquila Advisory – protecting you and your business

**Choosing the right adviser can be critical in reducing risk and protecting your critical personal and business data. At Aquila our experts are on hand to quickly identify vulnerabilities, highlight the risk to you of cyber crime and fraud, and to implement robust plans to protect your business.**

**To find out more about the services provided by Aquila Advisory, speak to us today. We will advise you of your options and to help you make the right decisions for you, your employees and your business.**

### **CONTACT AQUILA ADVISORY:**

**Jane Fowler, Managing Director**

Tel: 020 7397 8318  
Email: [info@aquilaadvisory.co.uk](mailto:info@aquilaadvisory.co.uk)  
Website: [www.aquilaadvisory.co.uk](http://www.aquilaadvisory.co.uk)

