encription
IT Security and Forensic Services

With IT security threats ever more prevalent, and the constant stream of information from the media about "Heartbleed" and "GoZ", how do you know if you, or your Company, are truly safe online?

In truth, there is no way to guarantee 100% security online, in fact, the only way to make sure that you don't get hacked, is to come off computers completely!! Even then, as hackers get smarter, and techniques develop, social engineering means that no-body is safe.

Statistics indicate, in fact, that over 30'000 websites report hacks per day (Source - Sophos Labs), and those are just the ones that have teams of specialists dedicated to detecting these intrusions, and are willing to disclose them. Moreover, from what we have learned about "Heartbleed", the reality is, that Companies, even when they know their services are vulnerable, are unwilling to disclose this to the clients, often for days, months, or even years after the vulnerabilities are discovered.

SO HOW DO YOU PROTECT YOURSELF?

Aside from living in a small hut in the middle of the Amazon rainforest, all you can do to try and maximise your security and to be smart online, by following some simple practices.

PASSWORDS:

We all hear from time to time about how our passwords should be longer, smarter, and more abstract, and this is never as true as after each big security breach.

Figures released last year show that around 92% of users re-use the same password for multiple accounts, and 80% of users have a password within the top 10'000 known passwords. Which means that if one site has a massive leak of passwords, like E-Bay, then a hacker can try those passwords against any number of other accounts, from Emails and Facebook, to banking, and even hacking into your own computer.

A lot of people will tell you that p@ssw0rd is secure, nobody is likely to guess it, and with the use of symbols, plus 8 characters long, it would seem fairly safe. However in reality, a password, such as "Eating Passive Pages Ketchup" is much more secure. "1337" speak may help, but 4 random words in a nonsensical order is much less likely to be in a hackers password list.

Changing your passwords regularly also helps, so that even if an attacker does gain access to your accounts, then you can limit the amount of time they have access for, before you lock them out again. This is vital if you want to ensure long-term protection.

TRUST:

You should never trust anyone with your password, regardless of how well you think you know that person, but trust does only apply to this.

Being able to verify a source of a website, and knowing that the vendor is someone you can rely on, and someone who you know will maintain integrity, means that you can circumvent a lot of the issues that come with "Phishing" attacks, where a person, or persons, using social engineering to try and trick you into giving them information.

We've all heard by now, about attacks such as the Nigerian Prince who wants to share his fortune, all he needs is your bank account information, pin number, and sort code. However, the advances made in the hacking world, mean that attackers don't even need to trick you like this. All they have to do is get you to go to a site, which looks identical to the one you're familiar with. However, when you type in your information, it is relayed on to them.

To avoid this, always check when you are using a "secure" site, that it is what it purports to be. To do this, in your browser, in the URL Bar, there should be a little padlock which tells you that that site has been independently verified as secure.

You should never go to a site you need to trust by following links. If, for instance, your bank sends you an email, don't follow the link on that, but instead, type in the banks web address in manually.

FIREWALLS & ANTI VIRUS:

As well as human intervention, computers can be configured to help fight against the threat of online security breaches. A well set up system of up-to-date Anti virus, as operating system with the latest patches installed, and a firewall controlling the traffic coming in and out of your network to ensure it is all legitimate, will mean that you should be relatively secure.

PENETRATION TESTING:-

The real problems with security occur when these practices are not followed. Any weak point in the chain can lead to a vulnerability, and if it is discovered, then a system can be hacked. This is what has happened with "Heartbleed", "Game over Zeus", and almost every other big security breach in IT.

Therefore, a good way to discover these problems is to have your systems tested. Have someone pose as one of these hackers, and get them to find your problems for you, before someone else does. Then, you will be able to fix the problem, and any gaps in your security can be fixed.

REMEMBER:

As good as a well configured system can be at circumventing security systems, there is no substitute, and no way of guaranteeing a systems security unless the people who use the system follow safe practices.