RESOLUTION IT

Cyber Security

In today's connected world, security is an ongoing process, not a point-in-time solution. Our goal for this document is not to frighten, but to inform and provide our clients with practical advice that will help them adjust practices to prevent any attack. Cyber-crime is now part of organised crime including; blackmail, sabotage and terrorism.

Recent examples include TalkTalk who were held to ransom for their data by an external hacker. Media generally only cover large multinationals, however lots of SMB's have been affected but don't generally make the media. Scottish hairdressing firm "Ellen Conlin Hair & Beauty" which has salons in Glasgow and Giffnock said it paid 1,000 euros through a third party after its system was hacked in October 2015. The hackers had locked its database and threatened to delete information, The firm said it decided to pay because it could not afford to lose business.

SMB's are most targeted because their modest security budgets make them more accessible and through these SMB's the supply chain of larger companies can be affected which, in turn, makes them vulnerable to extortion.

Insurance cover may in the case of many SMBs be inadequate or inappropriate for the risk that they have not anticipated. Location is not a barrier; therefore, any business can be targeted from all over the world. Attacks that occur outside the territorial limits of most insurance is unlikely to be covered.

Resolution IT can provide Enterprise Firewalls as-a-service from £65.00 per month which can significantly improve the security of the network. We would advise you to consider these Firewalls, so please don't hesitate to contact a member of the team who can assist in ensuring your network is safe.

However, no matter what security measures are in place, technology can only protect so far. There will always be a human element so education for everyone is key.

Ransomware and Cryptolocker

Ransomware is a form of malware/Virus that gives criminals the ability to lock a computer from a remote location. It then displays a pop-up window informing the owner that the computer will not be unlocked until a sum of money is paid. In some cases, the only usable part of the computer is the number keypad to enter a PIN to enable payment to the criminals. The best-known variety of ransomware in recent times is called CryptoLocker.

Although CryptoLocker itself is readily removed, files remain encrypted in a way which IT engineers find impossible to break. Many IT consulting companies advised clients that the ransom should not be paid, but did not offer any way to recover files; others said that paying the ransom was the only way to recover files that had not been backed up. Some victims claimed that paying the ransom did not always lead to the files being decrypted.

Resolution IT and leading IT Industry sources believe that CryptoLocker variants are one of the most prominent threats to the SMB. The landscape has significantly changed from viruses causing nuisance to international well organised 'professional' criminals aiming to generate large financial gain and possibly funding terrorism and other illegal activity. In December 2013 ZDNet traced CryptoLocker in an attempt to gauge the operation's financial takings estimated to be US $27 million at that time.
Because of the success of illicit financial gains seen in 2013 we have seen an increase in this type of Cyber threat with further variants. Dell SonicWALL reported detecting 55,000 new malware variants per day in its Dell Network Security Threat Report 2013.

Phishing

Phishing is a form of email scamming where cyber criminals pretend to be credible companies such as banks, credit card companies, online shops ands other trusted organisations. They will generally ask you to go to a website and fill in personal security details. The link is fake but designed to look exactly like the real website. This is to encourage potential victims into surrendering their personal information.

The email itself can also look as if it comes from a genuine source. Here's what to watch out for:

- The sender's email address is different from the trusted organisation's website address.
- The email is sent from a completely different address.
- The email does not use your proper name, but a non-specific greeting such as "Dear customer."
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format. The image contains an embedded link to a bogus site.

Protect yourself

- Do not open or forward emails which you suspect as spam.
- Do not open attachments from unknown sources
- Keep your spam filters on.
- Turn internet spam blocking on.
- Always 'hover over' a link before clicking on it to check that the link is taking you where you think you are going.

By hovering over links BEFORE clicking, the actual link will appear – check the link that shows up in the grey box is the same. If not, this is likely to be an unsolicited link and DO NOT click on it.

Passwords

Creating appropriate passwords and protecting them will dramatically improve your cyber safety. Strong, unique passwords will give you the best security.

- The longer it is, the harder to guess or break.
- Write a word you'll remember replacing some letters. with numbers or symbols: SP1D3Rm@n
- Pick the line of a song or saying and take the first letter of each word.
- Don't recycle passwords – keep them different.
- If you need to write them down, encrypt them in some way that only you understand.

Avoid using:

Your name

Your DOB

Important dates

Any family member or pet name

Hobbies/sports team name

Your hometown

The same password

Top 10 worst passwords!

1. password
2. Password1
3. 12345678
4. letmein
5. qwerty
6. 000000
7. iloveyou
8. trustno1
9. abc123
10. access

Best practice for everyone

Please remember that each user is the first line of defence and your 'cyber safe' behaviour makes a huge difference.

- ✓ Daily, weekly and quarterly backups.
- ✓ Don't ignore software updates.
- ✓ Make sure your anti-virus software is active.
- ✓ Report anything suspicious.
- ✓ Keep your web filtering active.
- ✓ Choose strong and different passwords.
- ✓ Email and internet safety. Ignore unsolicited emails, be wary of attachments and avoid untrustworthy (often free) downloads from freeware or shareware sites.
- ✓ If in doubt please ignore the message and seek advice.

Cyber Security Checklist for Management

- ✓ It's a board room issue and responsibility rests there. This is no longer just the remit of the IT Department so a board room approach needs to be enacted.
- ✓ Attribute a value to your companies' data – once the worth is realised, protecting it will seem obvious and cost effective.
- ✓ Get a security audit to include a 'gap analysis' to understand the true risk.
- ✓ Consider both internal and external risks; a disgruntled employee or rogue administrator are just as dangerous as an external hacker.
- ✓ Understand your personal risk as a director or manager and what your responsibilities are.
- ✓ Ensure your partners have appropriate protection in case your business is targeted as part of a supply chain. The risk is not just to your data. If you fail to take basic steps to protect client confidential information and they suffer, they can sue you for breach of contract.
- ✓ Educate staff regarding cyber security and let them know their responsibilities. There is no uniformity of insurance policy coverage so make sure that cover is what you need and that exclusions do not leave questions about where the damage has been done. Many criminals are working from outside the normal insurance territorial limits.
- ✓ Continued reassessment to ensure the right protection.

Further resources

Resolution IT highly recommends that directors, management and staff take time to ensure that they are aware of the cyber risks to their business and future job security and take appropriate measures and procedures to minimise the very real risks that exist today.

We have outlined some of the threats and ways to protect yourself but can only briefly cover the subject. Resolution IT publish security bulletins via social media and suggests you follow these to keep up to date on the latest threats.

We also suggest viewing www.getsafeonline.org which has lots of useful information.

Take this useful online quiz to see how 'safe savvy' you are: www.getsafeonline.org/quiz

+44 (0) 1481 267338
sales@resolution-it.co.uk