But as with driving a car, if we don’t take care when using technology then something can – and usually does – go wrong. How do computer viruses get onto an IT network? In the majority of the cases the virus-infected computer or network is typically caused by one thing – human error. Whether through haste, carelessness or simple ignorance, it’s your own users who pose the biggest everyday threat to your IT health. And if your technology systems then sneeze, your business can catch a serious cold.

A virus infection on your system could lead to widespread disruption and a loss of customer data. Viruses can steal your password and identity for fraudulent purposes, delete or corrupt important files or make your computer completely unusable until you pay a ransom demand. For groups of computers connected on a network, that virus can spread like wildfire internally and even be passed on to your customers or suppliers.

Mitigating virus risk is two-fold.

• Technical - a sound anti-virus system kept up-to-date along with a firewall.
• User awareness - the dos and don’ts of IT health – that’s backed by easy-to-follow processes. In this bulletin, we take a look at the common sense steps you can take to help keep damaging viruses away from your IT systems.

The scale of the problem...

At Arthur J. Gallagher we block over 800,000 email viruses, scams, malware and malicious web sites that pass through our IT systems each month. However these attacks are adapting faster than the systems being developed to prevent them and with over 20,000 employees, we naturally go to great lengths to protect our hardware, software and data. Our most important solution though is constant vigilance - making sure that our people are aware of the cyber risks we face and how they can help minimise those risks. Malicious virus developers and cyber criminals work faster than firms can defend themselves.

Remember:

- The internet is evolving and expanding – and that means heightened malicious virus activity on the web.
- Viruses are created before the specialists develop the anti-virus response, creating a window of vulnerability.
- The main route for a virus entering your IT system is accidently by a member of staff.
Where do you start? Cyber awareness training.

Working with security specialists Cyber AMI, Arthur J. Gallagher has developed essential cyber safety guidance that you can circulate to all your people to help better protect both systems and company against virus infections.

Recognising a potential virus...

A virus is a file or piece of computer coding that has the sole intention of doing harm or to carry out criminal activity – they can infect your computer through:

1. Opening an infected email attachment (eg Word or Excel document, .exe files).
2. Opening an infected file from a file delivery service (eg Dropbox, YouSendIt).
3. Clicking on a web link in an email.
4. Visiting legitimate but corrupted web sites.
5. An infected USB/memory stick that you then plug into a computer.

The following is an example of a virus-infected email received. The email has a fake sender email address and an infected ‘invoice’ Word document attached. It’s pretty convincing and all too easy to release on to your equipment and systems – with potentially damaging results.

Don’t get infected: our Do’s and Don’ts...

- **DO NOT** open files attached to emails from unknown, suspicious or untrustworthy sources.
- **DO NOT** click on links in emails from unknown, suspicious or untrustworthy sources.
- **DO NOT** click on ‘unsubscribe’ links in emails: these often lead to you being targeted more.
- **NEVER** download an unauthorised application from the Internet to a device you use for work purposes. Speak to your IT manager about your software needs.
- **DO** choose strong passwords using combinations of letters, numbers and special characters – not your birthday! Keep the passwords stored safely and separately – not on your computer.
- **DO** back up your data regularly – you can retrieve it if the worst should happen.
- **DO** install anti-virus software at home and keep current with subscription updates – they’ll update automatically. Vendors such as McAfee, Trend Micro and Kaspersky Lab offer protection for PC and Apple Mac.
- **DO** use the built-in firewalls that come with today’s PCs and Apple Macs – they’re easy to activate and will stop your computer being scanned by a malicious third party across the internet.
- **DO** be careful with USB drives (e.g. memory sticks) as they are a common carrier of viruses.
- **DO** delete suspicious emails.
- **REMEMBER**: scammers, spammers and hackers piggyback on trust. If you receive an email purporting to be from a client, supplier or customer, bear in mind it may still be fraudulent - so approach with caution.
Arthur J. Gallagher: our conclusions…

Whilst strengthened security procedures, good digital housekeeping and high user awareness will reduce the likelihood of your business suffering from a virus, it does not guarantee you will not be hit. In this case, having cyber insurance in place can help you deal with:

* The cost of discovering what has infected your system - and then removing it.
* Identifying what information may have been compromised.
* Engaging with legal providers to help mitigate the effects of the breach with your customers and regulators.
* Lost revenue whilst you were unable to operate due to system failure.
* Claims from customers for losing their data or money

And if your understanding of cyber insurance leaves you a little unsure, then come and talk to us.

About Cyber AMI

Cyber AMI is a web-based platform that provides a logical starting point in understanding cyber risk. It can help your organisation understand cyber risk, identify where you may be vulnerable and what you can do to improve your security. Use of the platform will train your organisation to the UK Government-backed Cyber Essentials standard for information security. For more information on Cyber AMI please visit www.cyber-ami.com.

About Arthur J. Gallagher

Founded in 1927, Arthur J. Gallagher & Co. has become one of the largest, most successful insurance broking and risk management companies in the world. With extraordinary reach internationally, our parent group employs over 20,000 people and provides services in more than 140 countries. Outside the US we are known as Arthur J. Gallagher and wherever there is an issue of risk, we’re there for our clients. We are a business without barriers – working together to create solutions that drive value and competitive advantage for our clients. Our people, our depth of technical knowledge and our global reach will deliver unrivalled advice and coverage expertise.

WOULD YOU LIKE TO TALK?

For more information call us on
T: 0800 612 2278
E: ukenquiries@ajg.com
www.ajginternational.com

“We are vulnerable in the military and in our governments, but I think we’re most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. It’s not going to go away”.

Michael Mullen, former Chairman of the Joint Chiefs of Staff, US Department of Defense