Executive Business Support

professional association management

CASE STUDY

The 'Hit and Hope Attack'

Computer viruses have come a long way in recent years and hackers are now far more professional. Rather than being independent and working from a hidden room or basement, hackers these days are often part of an underworld criminal network. Therefore the potential damage and destruction that can be brought by virus attacks has grown significantly, and is not to be taken lightly. Protection of the highest level is critical and here at EBS we have ensured this is in place. We recently detected a virus and without this protection there would have been terrifying consequences for us all.

Scenario

It was an ordinary day at the EBS office on 6th July 2016. The morning came and went but then the afternoon arrived along with something that could have caused serious irreparable damage to your data and our business; a virus attack.

We were first alerted to the attack when two members of our team noticed they couldn't access files. It became clear very quickly that these files (and others) were rapidly becoming encrypted and being replaced by 'zepto' files. On raising the alarm all PC's were immediately disconnected from the network in order to contain the virus and prevent it from spreading onto other PC's.

The Solution

After removing the infected PC's from the network, they were completely wiped. But what about all of the work and information stored on them? Is it lost forever? At EBS we use a reliable back-up system called 'Backup Exec' which is secured independent to the main server. It is automated, encrypted and checked on a daily basis. Because of this, we were able to easily restore the data back onto the affected PC's once they had been reinstalled onto the network. Had it not been for the separate back-up, the data would have been completely unrecoverable.

The security protection and procedures that we have in place here at EBS, combined with the swift actions of our team, stopped the virus attack in its tracks. Considering the strength of the virus, business continued as normal and within 48 hours all traces of the virus had been removed. There was no loss of data nor was there any interruption or disruption to the service we provide - you probably didn't even notice there was anything happening! Situations such as this can happen to anyone at any time and your investment in our services keeps you, your business and your members safe.

FACT: During 2016 our security systems blocked 133,991 suspicious e-mails and also prevented 892 viruses.

General Good Practice Guidance

- Don't ever say "it won't happen to me". It could.
- Use high strength passwords. Don't ever write them down and don't share them.
- Don't leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time, no matter how short, lock it up so no one can use it while you're gone.
- If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.
- Be wary of incoming emails and their attachments, if something doesn't look right then either delete the email or get it checked by an IT professional.
- Take the approach: 'if in doubt delete' as this is much safer than the 'open it anyway' approach.
- If you accidentally delete an important email chances are the sender will phone you or send it again. If you open a virus the consequences can be a lot worse!
- Back up your data regularly, and make sure your anti-virus software is always up to date.
- Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
- Be wary of social engineering and attempts to gain information from you through manipulation.
- Monitor all of your accounts for suspicious activity.

Executive Business Support Ltd
City Wharf, Davidson Road, Lichfield, Staffordshire, WS14 9DZ
01542 442140 ~ www.execbs.com ~ enquries@execbs.com