jwHinks

CHARTERED ACCOUNTANTS

Cybersecurity Handbook

The number one threat

Cybercrime is a big business. One in five companies are targeted every year, resulting in losses of more than £1 billion. And for charities the story is no different. Experts suggest that the not-for-profit sector is being increasingly targeted by cybercriminals because it holds a huge amount of data.

Cybercriminals are notoriously difficult to track, meaning they're very rarely caught. That's why charities should be prepared to prevent an attack before it's too late. In this handbook, we'll show you how unsecured networks, uninformed employees, and loose communication can set your charity up for a digital disaster.

What is phishing?

Some websites, emails, or phone numbers can look like they're part of an official organisation or that they provide more support than they do. Communication which masquerades like this is called 'phishing'. Its job is to spoof the respondent into handing over confidential details, such as a password or bank pin. The cybercriminal can then use these details to hack into an account and steal assets.

For example, a common phishing scam may include a hacker sending a spoof email from a bank asking you to look into "unusual" transactions. Other, less obvious scams may include the fraudster posing as a company director asking for funds to be transferred. This is called "spear phishing".

What is ransomware?

Ransomware is a type of malware that hijacks a computer and demands payment to release it. The hijacker will typically ask to be paid in cryptocurrency, such as Bitcoin.

This is because virtual currency is exceedingly hard to track. On most occasions, the hijacker will threaten to delete the victim's data if they fail to make a payment. However, there is no guarantee that the victim's files will be returned once payment has been made. Some types of ransomware will deploy a countdown timer, which might give the victim anywhere from one hour to one week to pay the hijacker. Ransomware is commonly downloaded onto a computer by mistake via an email attachment, or through unsafe web pages.

What is a virus?

A computer virus is designed to quickly spread from host to host, stealing data or destroying everything in its path.

Some viruses can be stealthy, while others are purposely malicious. A virus may also be capable of relaying information about your computer in real-time. For example, a 'keylogger' virus is able to track every keystroke typed by the end-user. Viruses are typically downloaded in a similar fashion to ransomware – either through email attachments or unsafe websites.

Education is key

Your antivirus software might be the best in the world, but it's only ever as good as the team that uses it.

Fraudsters will deliberately attack the most vulnerable, so it's vital that you ensure your whole team is up to scratch on preventing cyberattacks.

What to do in the event of a cybercrime

1. Do not panic

It's easier said than done, but stressing about the consequences will only make things worse.

2. Disconnect from the internet

That way, the hijacker will no longer be able to contact you or your computer.
Anyone else on the network should disconnect from the internet too.

3. Contact your IT support provider

Get in touch with your experts to help you and make them aware of your problem. If you do not have one, contact us and we can recommend some experts who can help.

4. Change passwords using a different network

For example, you could use your smartphone's mobile data (providing it hasn't been connected to the affected network). You should also contact your bank account provider if you suspect it may be at risk.

5. Scan your computer using antivirus software

If you're unable to remove the threat you should seek expert advice.

6. At this point, it may be necessary to reinstall your operating system to the latest back-up

Don't have a back-up? That's why you have to follow our cybercrime prevention checklist (before it's too late!)

Cybercrime prevention checklist

☐ **Create regular back-ups**

Ideally, your network should be backed-up at least once a day. You can use specialist software to do this for you automatically.

☐ **Enrol the help of an anti-virus**

An anti-virus quietly works in the background, scanning email attachments for potential attacks or alerting you to harmful web pages.

☐ **Update your computer**

Don't ignore the update alerts for days on end – they might contain a patch protecting you from a newly discovered exploit.

☐ **Team training**

Anyone using a computer on your network should be equipped with the knowledge to prevent a cyberattack. Implement policies which you think could help your organisation stop an attack before it happens.

About JW Hinks Chartered Accountants

The team at JW Hinks draws together expertise from various disciplines, and so has the skills required to provide support and advice to a range of businesses and organisations.

Furthermore, we are dedicated to getting to know each of our clients individually, in order to best serve their needs and those of their businesses. We act for a large number of businesses and organisations across a wide range of sectors. As a result, we can really make a difference, regardless of the size of your organisation.

JW Hinks LLP 19 Highfield Road Edgbaston Birmingham B15 3BH
T: 0121 456 0190 **F:** 0121 456 0191

Chartered accountants & lawyers
UK 200 group

info@jwhinks.co.uk • www.jwhinks.co.uk