TECHNOLOGY INSIDER

Find out How To Protect Your Business from Cyber Crime

Attend our Cyber Security Workshop.

This is an in-depth workshop session which will last approximately 2 and a half hours and be held at our offices in Eastwood, Nottingham.

It is aimed at business owner/ decision maker level and will focus on some practical steps that you can take to improve the basic security in your business, whilst explaining the additional steps you may need to look at for compliance and insurance.

Identifying the Problem
- Who and what is the biggest risk to your business?
- Where are your weaknesses?
- Calculating the cost of a cyber-attack for your business and how much you'd be willing to pay a hacker?

Taking Action
- How to conduct a Cyber Risk assessment
- How to keep staff up to date and enforce a secure culture in your business
- How you can sleep tight knowing your business is monitored 24/7

Due to the nature of this workshop we can only accommodate small numbers and are offering them on a strictly first come, first served basis.

If you would like to reserve a place please book via Eventbrite by following the link below

https://tinyurl.com/ cyber-workshop

DID YOU KNOW...
paying ransomware makes you a bigger target?

Ransomware is evil. It's where your data is encrypted until you pay a ransom fee to get it back.

Many business owners say they'd pay the fee to resolve the problem quickly. But doing that can make your business an even bigger target for attacks.

80% of ransomware victims who paid up were then hit a second time by the same attackers.

Doh.

The greatest defence against ransomware is being 100% prepared. You need a working and verified backup, a ransomware resilience plan, and all the right security measures in place **BEFORE** you are attacked.

Technology update

Business Email Compromise (BEC) attacks have grown into a £35 billion a year industry.

That's where someone gets into your bank account or systems through your email. Cyber criminals are trying to get you to click a bad link so they can steal passwords or install software on your computer.

Between July 2019 and December last year, business losses due to email scams grew by 65%.

You can't use software alone to protect your business. You need a blend of security tools and staff training.

Do you think your business could be vulnerable through email? Most are.

We can help. This is what we do. Call us.

INSPIRATIONAL QUOTE OF THE MONTH

"Technology will never replace great teachers but technology in the hands of great teachers is transformational."

George Couras, Innovative Teaching, Learning, and Leadership Consultant

TECH FACTS

#1
As people become more suspicious of technology, new phobias develop. Technophobia is the fear of technology and cyberphobia is the fear of computers

#2
Want to know how old you were when the internet was born? Visit www.howoldistheinter.net

#3
In the 1950s, computers were called 'Electronic Brains'. Shall we stick with 'computer'?

WHO WILL GET THIS MONTH'S TECH QUIZ CROWN?

You do have a tech quiz crown, right?

1. How many programming languages are currently in use?
2. What's the name of a website designed just to be used for sharing information inside a company?
3. Which mobile operating system does Google control?
4. What does PDF stand for?
5. What is a computer trojan a form of?

The answers are below.

1) It's really hard to say. Wikipedia has a list of about 700. But some programmers claim there are up to 9,000 languages in active use
2) An intranet
3) Android
4) Portable Document Format
5) Malware

Are you blacklisting or whitelisting?

You know what it means to be blacklisted, right? (we don't mean through personal experience, of course).

Blacklisting is where you block something you don't trust. It's used to keep networks and devices safe from bad software and cyber criminals.

But there's another, safer way of doing that – and that's called whitelisting.

Rather than trying to spot and block threats, you assume everyone and everything is a threat, unless they've been whitelisted.

But which is the right approach when it comes to keeping your business data safe? This debate rages on, with many IT professionals holding different views.

Here are the main differences...

- Blacklisting blocks access to suspicious or malicious entities
- Whitelisting allows access only to approved entities
- Blacklisting's default is to allow access
- Whitelisting's default is to block access
- Blacklisting is threat-centric
- Whitelisting is trust-centric

There are pros and cons to each approach. Whilst blacklisting is a simple, low maintenance approach, it will never be comprehensive as new threats emerge daily. It's also easy to miss a threat, as cyber criminals design software to evade blacklist tools.

Whitelisting takes a stricter approach and therefore comes with a lower risk of access.

But it's more complex to implement and needs more input. It's also more restrictive for people using the network and devices.

Confused? You're not alone! If you'd like to discuss which approach is best for your business, get in touch.

Q: How can I avoid being phished?

A: The best thing is treating every email with caution. If you're unsure, check the address it's been sent from, look for grammatical errors, and see if the layout looks like a normal email from that person or company. If you're unsure, don't click any link.

Q: What's an insider threat?

A: It's the name for when someone within your business gives cyber criminals access to your devices or network. Usually it's not malicious. But it's why regularly training your team in cyber security is a must.

Business gadget of the month

If you want to upgrade your webcam without spending a lot, you can use your phone's camera. You also need a good tripod to hold it.

The Joby GripTight ONE is a great option. It's under £50, has bendy, flexible legs, magnetic feet, and is small enough to carry from home to the office.

Q: How do I choose the right backup for my data?

A: Security and reliability should be your main considerations. Get in touch and we'll tell you what we recommend.