Bob's Business

REMARKABLE REALITIES

CYBERSECURITY EDITION

Does the thought of setting up multi-factor authentication bring on a migraine?

Do stock images of hackers in hoodies strike fear into your heart?

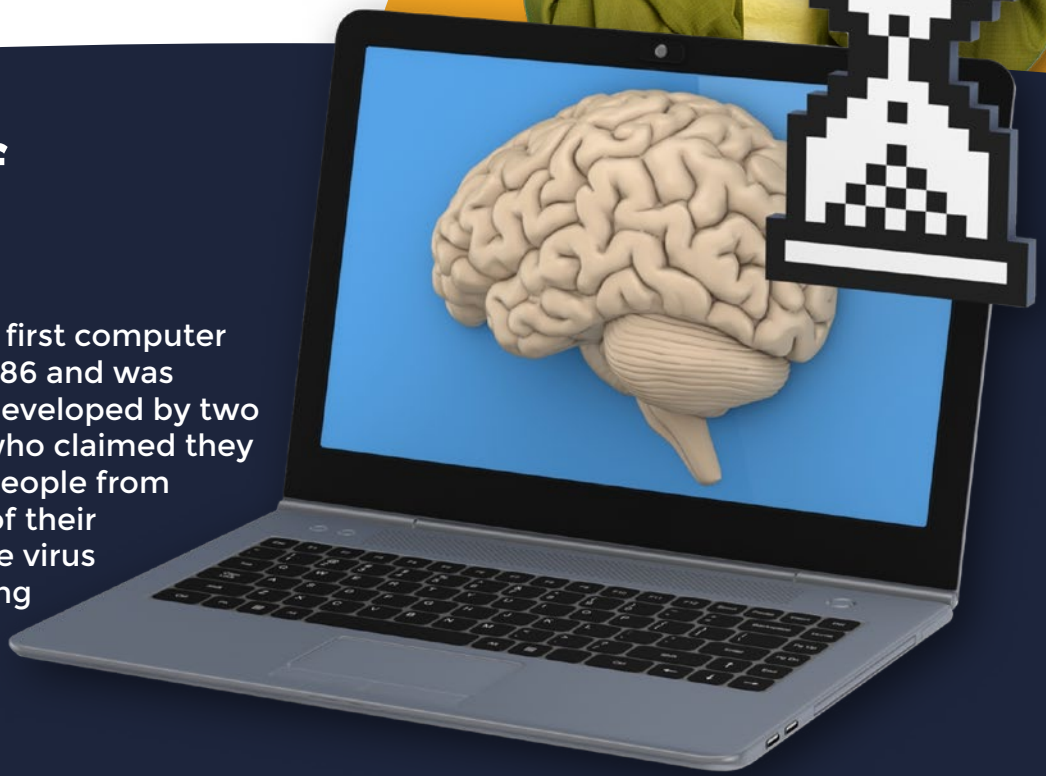
Have you ever thought, 'if only there were an informal guide to cybersecurity, focused on the weird and wonderful'?

Well, you're in luck!

We know the cybersecurity world can feel intimidating - especially if you're only at the start of your cybersecurity education.

At Bob's Business, we believe in demystifying cyber and making cyber education fun, approachable and - above all else - engaging for individuals and employees alike.

In this guide, we will dive into some unusual facts and statistics we've encountered over 15 years of working to reduce risk across businesses. Let's get started!



Attack of the Brain

Did you know that the first computer virus was created in 1986 and was called "Brain"? It was developed by two brothers in Pakistan, who claimed they created it to prevent people from making illegal copies of their software. However, the virus quickly spread, infecting computers around the world and causing chaos.

Bob's Business

Puny Passwords

Passwords are often the last line of protection between cyber criminals and our accounts, but you'd be amazed at how often these passwords are easy to guess.

The top five most common passwords of 2022 were:

123456
password
liverpool
password1
123456789

Spotted your password in that list? Consider this your polite warning to secure your accounts as soon as possible.

Want a quick and easy way to build a strong password? Pick three random but memorable words and augment with numbers, like Vortex8King3Moth.

The Chaos Computer Club

Germany is home to Europe's largest association of hackers who have been hacking for over 30 years for good! They have a strict policy of not attacking individuals or organisations for financial gain. Instead, they use their skills to expose security flaws and raise awareness of cybersecurity issues.

MyDoom

Thought computer viruses were just a minor annoyance? Think again. In fact, one virus in particular - MyDoom - is the most expensive virus in the history of cybersecurity!

This insidious piece of malware caused an astonishing $38 (£31.5) billion worth of financial damage, making it one of the most destructive cyberattacks ever. MyDoom first appeared in 2004, and quickly spread across the internet, infecting countless computers and causing chaos in its wake.

Laser-powered Hacking

Although human error is the most common cause of a breach, it's not just humans who can be hacked.

In 2017, a team of researchers from the University of Michigan and the University of South Carolina hacked into a smart speaker using a laser beam. By shining a laser at the speaker's microphone, they could trick it into registering sound, even though there was no actual sound in the room!

The Kids (Aren't) Alright

Believe it or not, the myth that older people are more at risk of cyber attacks is just that - a myth. In fact, according to the Norton Cybersecurity Insights Reports, it's actually millennials that are the most vulnerable when it comes to cyber-attacks.

It might seem counterintuitive, but the truth is that 44% of millennials have fallen victim to cyber-attacks - often by sharing passwords for something as harmless as Netflix, or as sensitive as a banking password. Despite growing up in the digital age, many millennials are still unaware of the potential risks associated with sharing passwords, and this can leave them open to attacks from cybercriminals.

Social Engineers at Work

Social engineering might sound like a round of drinks down at the site, but the reality is vastly different! Social engineers utilise a wide variety of persuasion and habit-based techniques to gain access to your data.

From phishing and baiting to pretexting and impersonation, click here to read our full guide on social engineering!

The Fishtank that Hacked a Casino

Search engine phishing is a relatively new phishing technique that involves the fraudster creating a legitimate-looking website that features in search engine rankings - often in the 'shopping' section of a search query.

The website will typically offer amazing deals, but when the website user pays for their order the products never arrive. The payment details might also be used for further fraudulent purposes, such as making big purchases.

You WannaCry?

Government-made malware is a very real thing, and it's had shocking consequences! One of the worst examples of this attack is the leaked NSA exploit EternalBlue, which ultimately led to the spread of WannaCry, one of the worst ransomware attacks in history.

How Bob's Business can help protect you and your organisation

Whilst the world of cybersecurity might feel impenetrable, the reality is that 90% of breaches occur due to simple human error.

The solution to those errors is training, but not just any training.

At Bob's Business, we make training fun, approachable and, above all else, truly effective.

How do we do that? By making seemingly complex topics like cybersecurity and compliance into easy to understand through real-life stories, humorous animations and actionable advice that anyone can utilise.

When everyone on your team understands their role in spotting and stopping attacks, that's where positive cybersecurity culture begins.

Ready to learn just how affordable and effective training from Bob's Business can be? Click the button below and book a slot with a member of our team.