Welcome

CYBER-CRIME. DATA BREACHES. Identity theft. A decade ago, these concepts were barely considered by the web-surfing public; but today they're all too familiar a concern.

As we migrate an increasing amount of our personal and professional lives to the virtual world, so too grows the threat to our data privacy.

Security breaches can disrupt our lives – sometimes irreparably – so its understandable that many feel helpless in the wake of cyber-crime. Pulling the plug on our data, however, simply isn't an option given how entangled our lives are in social media, banking apps, messaging and other modern 'essentials'.

Instead, as the experts say, it's incumbent on us all to do the basics right. The harder we all make it for the bad guys, the better chance we stand of continuing to get the best out of our lives, wherever we may roam. So how to do that?

Did you know?

£1.2tn

Amount lost to cyber-crime in 2018

KEEPING CYBER-SAFE AND CYBER-SOUND.

With online security threats ever-increasing, the question on every web-user's lips is: what can we do to reduce our risk? *Simeon de la Torre* reports

If you were looking to list mankind's greatest achievements of the past 50 years, then it would be difficult to ignore the internet, alongside its close relation the World Wide Web. In the three decades since British engineer Tim Berners-Lee first conceived this system, initially devised as a means for scientists to share information over great distances, the web has gone on to change the world – revolutionising the way we live, love and work. But as it has become more ubiquitous, its ability to impact our lives in every way has also grown.

The worldwide cyber-threat is on the increase all the time – according to IT security business Yubico, more than 3.8 million records are stolen every day from data breaches, 80% of those due to stolen or weak passwords. The cost to businesses in IT support alone is staggering – password resets can cost large enterprises nearly £10m per month, the firm estimates.

Small businesses are at threat too, especially because they're less likely to have dedicated security departments or full-time IT teams to help police their networks. So, how to protect yourself?

ENTRY POINT

The most common way that attackers gain access to your personal data is through your email – a process known as phishing. John Higginson, head of incident preparedness at Context Information Security, explains: "People should look out for emails from people or organisations they don't know, or from people they do know but are not expecting." If you've ever received an email with an invoice attached when you haven't ordered anything, or an email purporting to be from a manager or service

IMAGES GETTY

provider, they are common ploys too, he says.

Other tell-tale signs may be that your computer is acting a bit weird or is a lot slower than normal – if in doubt, get it checked out.

In a 2019 survey by cybersecurity firm SureCloud, 63% of people were most worried about being compromised by a targeted phishing attack. The firm's operations director Luke Potter says the issue shouldn't be left to

"PEOPLE SHOULD LOOK OUT FOR EMAILS FROM PEOPLE OR ORGANISATIONS THEY DON'T KNOW, OR FROM PEOPLE THEY DO KNOW BUT ARE NOT EXPECTING"

the techies to fight: "It is critical that organisations adopt a 'top-down' approach to cybersecurity, meaning that engagement is gained at executive and board level for cyber-resilience and that it is propagated throughout the workforce. Cybersecurity is the responsibility of everyone in the company, not just the IT or information security team – we all have an obligation."

ON THE MOVE

The good news for travellers is that we shouldn't necessarily regard any locations as off-limits, or more of a risk. It's simply important to exercise extra caution whenever you're using an unprotected connection – even in your home city.

Luis Corrons, security evangelist at Avast, advises that Virtual Private Networks (VPN) are essential for anyone connecting to a public WiFi spot they are not in control of. "A VPN creates a secure encrypted connection, protecting personal data and preventing hackers from accessing or even altering communications over the internet.

"If you imagine a neighbourhood with spies on every street corner tracking your movements from one house to the next, a VPN is like your own private underground tunnel that connects you to each house and is beyond the view and jurisdiction of the spies. All they will see is that you left your house at X and returned at Y, but they cannot see which house – or website – you've visited."

Mobile tech isn't inherently more vulnerable than an office environment – as long as you're vigilant. However, Tamzin Evershed, chief privacy officer at Amex Global Travel, believes there are a few areas where greater care is required: for example, don't check anything on public WiFi that you wouldn't want anyone else to see.

THE SOCIAL NETWORK

"What are you revealing in your social media posts?" Evershed asks. "You can inadvertently reveal commercially sensitive information – for example, by posting that you are in New York for a business meeting, you might be revealing that your company is bidding for a particular contract.

While this is, of course, a concern it's also something that is easily addressed, if you follow the advice in this piece. By taking the appropriate measures, applying a little common sense and the same degree of caution that you would if you were talking in a public place in the real world, you can easily protect yourself. And that then leaves you to enjoy all of the manifest benefits that the online world has to offer.

"BY POSTING THAT YOU ARE IN NEW YORK FOR A BUSINESS MEETING, YOU MIGHT BE REVEALING THAT YOUR COMPANY IS BIDDING FOR A PARTICULAR CONTRACT"

IMAGES GETTY