

ReliableTech

Your Monthly Source of Trustworthy Tech Insights

Acknowledging risk & strengthening defences

Welcome back to Reliable Tech: your trusted companion for your digital journey.

This month, we want to take the opportunity to talk about digital security in even more detail. The fact is that attacks are becoming increasingly sophisticated, which means that the measures we're implementing today may not hold up tomorrow, leaving us vulnerable to risks in the near future.

And so, for our June edition of Reliable Tech, we want to do two things: ensure our readers are aware of the biggest risks they're likely to face, and understand how best to build stronger defences.

If that sounds like something you'd be interested in, keep reading!

Gone phishing?

Unfortunately, there's an almost never-ending list of ways cybercriminals can gain access to our data, or prevent us from operating as normal. Viruses, worms, ransomware, adware, spyware, trojans... you name it. And, of course, it's important that we're prepared for anything criminals may throw at us.

However, there's one type of attack that's more common than any other: phishing. Why? Because it's incredibly simple to orchestrate. All cybercriminals need to do is send an email, and hope that one of the recipients falls for the scam, clicks the link, and shares sensitive information via a fake website.

Phishing attempts can be very difficult to spot. But that doesn't mean they're impossible to thwart. We discuss some of the most effective techniques – like carrying out phishing simulations – in our recent blog post looking at powerful ways to protect your business from phishing attacks.



Did you know...



Almost 50% of UK businesses still don't have an agreed process in place for how to deal with phishing emails. Many employees aren't sure when to report suspicious communications – or who to report them to. This means that potential phishing attempts aren't being managed in the most effective way.

Making security simpler

To combat risks like phishing effectively, all businesses need to make digital security a firm focus. And that means getting everyone on board, and asking everyone to do their part to boost resilience. But there's a problem. For non-IT staff especially, cybersecurity can be a complex topic. We need to find ways to make security simpler, more accessible, and easier for everyone to embrace.

You can do all this, and empower employees, with Power Platform. Power Automate – part of Microsoft 365's Power Platform – is a top tool that automates security tasks to support every employee as they strive to work in a safer, smarter way. For example, the tool can automatically send an email when a security patch is released, prompting users to keep their digital systems up-to-date.

Embracing change

The truth of the matter is that, to safeguard against today's advanced cyber attacks, businesses must be willing to change. They need to be ready and prepared to implement new solutions, and embrace new ways of working that can give them a competitive edge when it comes to security.

Before embarking on this sort of change, however, businesses need to develop their own digital transformation strategy. This is a roadmap to success that clearly and transparently outlines why change is needed, how it'll be approached, and the expected outcomes. With a plan in place, organisations can ensure they're staying on the right track, and always heading in the right direction.

In the real world... Estate fund manager, Frogmore, wanted to reduce IT costs and streamline business processes, all while remaining as safe as possible in the online space. We stepped in to help them out with their digital transformation, carrying out a complete digital overhaul. This not only helped them secure their digital assets more effectively, but also saved them over £70,000 in ongoing IT costs.



[Read more >](#)

Eager For More?

We'll be back next month with the latest edition of **Reliable Tech**.

Can't wait? want to know more, contact your Reliable Account manager or contact us below



Inspirational quote of the month

"It's time for executives outside of IT to take responsibility for securing the enterprise. Ransomware and supply chain attacks... should be a wake-up call that security is a business issue, and not just another problem for IT to solve."

Paul Proctor,
Research Vice-President, Gartner



Top Tech Tips

Every month, we ask the Reliable team for their top tech tips to share with businesses.

1. Make your employees a priority

Businesses can do everything right when it comes to cybersecurity. They can have all the right solutions in place. They can have solid defences. But really, none of that matters if their employees aren't adopting secure workplace practices. Organisations should be making their employees a priority, ensuring they have what they need to work safely and securely.

2. Get buy-in for change

You may have heard that a lot of change initiatives fail. It's true. But don't let that put you off starting your digital transformation journey. One of the biggest reasons for change failure is simply that it's not clear to everyone why change is needed, what it will involve, and how it will impact operations. So before embarking on a change project, it's worth putting the work in to help everyone prepare.