New Year, New Cybersecurity Threat? …Not Exactly

For a lot of us, 2020 felt like it was never going to end, but now that unprecedented year is finally behind us, what does the future hold for us in terms of security? Is there a new cybersecurity threat on the horizon, or just more of the same? And how prepared is your organisation to defend against cyberattacks both new and old?

With each new year comes unique challenges, but it's safe to say that the upheaval caused by lockdowns in 2020 was a particularly large hurdle. Thankfully, many organisations either had the technology in place to switch to remote working quickly, or they adapted rapidly for the sake of business continuity. Now that 2021 is well underway, we hope that you've resolved to maintain robust security for the year ahead.

So, what attacks could you come up against? While the threat landscape has shifted and evolved quite a bit recently, the kinds of cyberattacks your organisation could face remain largely the same.

Ransomware

Ransomware is a kind of malicious software that infects a device, restricting access to the tools and files on it until a ransom is paid. If that's not scary enough, ransomware is one of the fastest growing threats in cybersecurity, with global damages predicted to reach £15 billion this year.

The threat of ransomware isn't slowing down, but is it changing?

In 2021, we expect to see cybercriminals exploit remote employees' use of home internet connections – which are often far less protected than corporate networks. This makes it easier for malicious actors to gain entry to an organisation's systems and cause all kinds of chaos. Attacks are also likely to grow in sophistication; instead of simply holding your systems to ransom until you pay, attackers could completely destroy your corporate data if you don't comply fast enough, or take copies of it and release it publicly. Seeing as a data breach is likely to be more costly – both in terms of finances and business reputation – more and more organisations will be forced to pay up.

Even if you do submit to these demands, that doesn't mean you're out of the woods entirely. What's to stop threat actors from demanding another payment later on? Businesses of all sizes are at risk, but 2021 will see an increase in "big-game hunting" – where criminals target larger companies that can meet higher ransom demands – so expect to see some high-profile organisations in the headlines over the coming months.

Phishing

Unfortunately, social engineering scams aren't going away either, they too are increasing and gaining in sophistication. If when you hear "phishing scam" you think of a barely coherent email, suspicious sender, and an obviously dodgy link – you need to think again, because social engineering has upgraded in a big way.

Scammers are taking full advantage of the ongoing global panic by creating pretty convincing emails that pose as COVID-19 alerts, vaccine information, and government advice. With the current lockdown stretching as far as March, and vaccine rollouts currently underway, we don't expect phishing scammers to change their tune anytime soon. 2021 will see phishers closely following news headlines in a bid to reach your inbox first, spoofing the NHS, your local council, and even the WHO.

The pandemic isn't the only crisis that threat actors will be exploiting in 2021; with financial uncertainty and political unrest still very much an issue, we expect to see a rise in emotionally targeted political phishing. Threat actors will target victims using polarising political messages designed to tug on your heartstrings or stoke anger. We also expect to see attackers spoofing causes and asking for donations – or impersonating political figures/parties that their victims not only trust, but are likely to advocate for.

With many employees still working remotely and relying on a plethora of devices, not just their office PC, smishing will continue to increase. By targeting mobile devices, attackers are after two things:

1. The sensitive data tucked away on your corporate device or BYOD phone.

1. Access to your organisation's 2FA, as the 2nd factor is often your mobile device, so once they have that, the possibilities are endless.

An increase in Spear Phishing – well researched, targeted phishing attacks – is also inevitable. We expect to see cybercriminals going after large targets with calculated campaigns and a full arsenal of spoof emails, text messages, and – as deepfake technology becomes more sophisticated and more accessible – even spoof phone calls and video calls.

Make Robust Security Your New Year's Resolution

Kickstarting 2021 with security high up on your list of business priorities will stand you in good stead for the rest of the year and beyond. We appreciate that when lockdown started, you may have flexed your risk appetite for the sake of business continuity, but now your business has had time to get used to the new normal, and it's time to reign in that risk.

When reviewing your security budget for the year ahead, don't neglect offensive security; testing the strength of your current security posture will give you a good idea of how secure your business currently is, and how to improve it. This isn't just a "one and done" solution

either; as you hire new staff, update systems, and implement new technologies over the course of the year, your environment changes. We recommend regular penetration testing to ensure that no vulnerabilities slip through the net as your business navigates the choppy waters of 2021.

We also recommend security training – when's the last time you ran a phishing scam simulation on your employees? It's even more vital to bring your staff up to date on the latest security threats, especially now that they're working from home and are outside of the safety of your corporate perimeter. One human error could be costly to your business, so empower all staff with security awareness training, but in particular, invest in upskilling your security team so they're prepared for anything a cybercriminal might throw at them this year.

COVID-19 isn't going anywhere, and unfortunately, neither is ransomware, or phishing scams. These are two enemies we all know well, and that knowledge is power: we know how to keep them at bay. Forward-thinking security companies are upgrading their tools and techniques at lightning speed, ready to tackle cybercriminals head on and defend your organisation. It's not just about investing in defensive security; offensive security is also part of the puzzle that all fits together to form an iron-clad cybersecurity strategy.

By starting 2021 with a focus on security, you can maintain your organisation's success for many years to come.

To protect your organisation from cyberattacks both old and new, please contact us for a discussion with one of our security experts.

It has been estimated that cyber-crime now costs businesses worldwide up to $6 trillion each year, that's twice as much as 2015's $3 trillion total. What's worse, by 2025, cybercrime is projected to cost organisations a whopping $10.5 trillion annually.

Cyber-criminals are only getting stronger, more advanced, and more prolific, which is why it's important for businesses to stay one step ahead. For some additional updated stats, check out this Toptal article.