CYBERFORT

COVID-19: PROTECT YOUR HOME AND REDUCE THE CYBER R NUMBER

An old Cyberfort proverb reads "Working securely doesn't stop at the office door" and, given our present situation, this has never been truer.

The concept of 'the office' has mutated far beyond recognition over the course of the last two decades. It has long ceased to be 'just a building'. The office, as we know it today, has no fixed location. Instead, we carry it with us in our pockets and laptop bags, between meetings and on transport, before bringing into our homes.

In light of the COVID-19 pandemic, there are millions (potentially billions) more of us working from home and ensuring our continued digital safety is crucial. The r number refers to the 'rate of infection' of a virus (how many people an infected person can infect) but it can also apply to a computer virus and other online threats. By staying safe and bringing this number down, we can reduce the chance of our actions impacting anothers digital safety.

Below, we have laid out our Three Pillars of Risk, all of which are essential

DATA SECURITY & PRIVACY

10M RISE

Businesses have rushed to move employees online to work from home. Zoom participants alone have increased from 10 million in December to 300 million last month.

RESPECT?

While the platforms and apps may be secure, you should also ask the question "is X respecting my privacy?". Is your business-critical data secure?

CONTEXT

Always consider the context of your conversation, regardless of your platform of choice.

ISSUES

ALL platforms have security and privacy issues. The topic you are discussing should determine the level of additional security required.

DOMESTIC TECHNOLOGY

ADOPT

The pandemic has forced us to adopt domestic technology that was never intended for business use.

RISK

"Many more 'consumer' devices

+

Diversifying use of platforms

=

Increased risk of Cyberattack"

Andy Simpson-Pirie, Group CTO

UTILISE

To help mitigate breaches, ensure you have strong best-practice security in place. Utilise 'multi-factor authentication' and verify guidance with a trusted partner.

INTEGRATION

Consider how you will integrate domestic technology with your organisational IT services.

PHISHING & MALWARE

CYBERCRIME

Cybercriminals have dramatically increased and diversified their operations to take advantage of the pandemic. Risk levels have greatly amplified.

400% EXCESS

Action Fraud has reported an increase of cybercrime in excess of 400%. We believe that for each incident reported, another nine are not.

126M

Hackers are also targeting health services, along with any and all sectors. Google recently blocked 126 million COVID-19 related phishing attacks. No one is immune.

BE SURE

Regularly run security scans, scrutinise internet links before clicking or logging in, don't download something if you're unsure, check that people are who they say they are. Vigilance is key.

WORK SAFER, WORK SMARTER

These three pillars of risk cover the essentials of staying safe online when working from home. Data security and privacy, domestic technology, and phishing attacks all have their own challenges. Use the advice here to keep your family, your employees, and your business protected.

Of course, there are many other varieties of cyber threats out there in the darker recesses of cyberspace, but the key is vigilance and common sense. Remember: work safer, work smarter.