How to stay cyber secure working from home

We wrote recently about the benefits of a fluid workforce and strong flexible and remote working practices, particularly poignant during the current national lockdown. Whilst many are offering their tips for best home working practices (exercise, take a lunch break, get dressed), there is a less touted issue surrounding remote working, one with potentially catastrophic ramifications: Cyber Security.

Principal recruiter Ben Craig, also Communications Director at Cloud Security Alliance, spoke with Francesco Cipollone of NSC42 Ltd to find out what we all need to be doing to stay safe online when working from home.

What is the risk?

Home networks are always under more threat than office due to weaker security postures.

Unfortunately, right now every hacker and cyber criminal in the world is very aware that everybody is working from home, so critical company data is theoretically easier to access.

The response has been a significant ramping-up of phishing scams and malicious website, claiming links to COVID-19, or posing as your employer needing to re-set your account. Long periods of isolation and general displacement being away from the office can make it easier to forget stringent measure and double (triple) checking, but now is the time to ramp up your security awareness, not relax it.

What are the common attacks?

Phishing

Phishing is cyber crime involving victims voluntarily giving access to bank accounts or personal data due to the belief they have been contacted by an official organisation (e.g. their employer or bank).

This often begins as an email which looks incredibly authentic, using correct logos and fonts, leading you to a website (also authentic looking) which asks for details. Once you fill these in the attacker has full access to them.

Other phishing scams include SMS and WhatsApp messages, phone calls, even fake invoices (often with a nasty bailiff threat attached.)

Malware

Malware (Malicious Software) is exactly what you would expect. Ranging from inconvenient to disastrous, malware does anything showing unwanted ads and pop-ups to accessing private systems and data.

Ransomware

Ransomware is a type of malware which encrypts users' computers and prevents them from accessing their data. The hacker will demand a ransom in exchange for decrypting your files, essentially locking you out of your computer until you pay up!

How can we avoid falling victim?

Keeping safe at home is really important and it doesn't need to be a daunting task. As NCS42 have already written about in this article, as a minimum you should:

- Check your home network
- Ensure you add multi-factor authentication (MFA) to everything
- Check any and all links you are emailed

A lot of this will have been taken care of by your employer, but if you're unsure of anything, contact your IT support.

Steps that you can personally take can be found in this SANS factsheet, summarised below:

Understand social engineering.

Hackers will use specific tactics to leverage information. At the moment this includes scaremongering around job loss and coronavirus.

- This often requires a sense of urgency, deadlines or fear.
- It may encourage ignoring security policies or an amazing offer.
- A message from somebody you know where the tone or wording is off.

Secure the home network.

- Reset the default administrator password.
- Set additional passwords for other users which are different to the admin.
- Create strong passwords, ideally using a password manager.

Password management.

- Re-set your passwords using strong passwords.
- Use a password manager to securely store them.

Stay up to date.

- Keep all systems and applications up to date with the latest versions and regularly check this.

Keep work & family separate.

- If you can set up guest options on your router make sure you do.
- Make sure family and friends know they cannot use your work devices for any reason and keep them out of reach of children.

NSC42

NCS42 can help to protect your business in this challenging time and they do so as community service.

They are also supporting the COVID-19 cybersecurity supporters initiative and were recently featured in Wired with Red Goat's Lisa Forte and Daniel Card from PwnDefend.

If you want to know if your businesses or your employees are safe during this period, or need some Cyber Security advice, get in contact with NSC42 for a free 30 minute, no commitment assessment.

communications@nsc42.co.uk

CSA cloud security alliance℠

The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing and provide education on the uses of Cloud Computing to help secure all other forms of computing.

The Cloud Security Alliance is comprised of many subject matter experts from a wide variety disciplines, united in their objectives.

Find out more:

http://www.cloudsecurityalliance.org

INFOSEC

InfoSec People are a boutique, ethical, cyber security and IT recruitment business. Based in the South West with national reach, InfoSec recruit both contract and permanent experts from board level to junior, based on the simple tenet 'great people for great companies.'

If you need advice or are looking to enhance your cyber security posture or grow you IT teams, or simply want advice on remote working, contact our team today for an informal discussion.

01242 507100
info@infosecpeople.co.uk