CYBER AWARE

south east
Regional Organised Crime Unit

Cyber-crime – A booming business!

Surrey & Sussex CCU Newsletter – August 2020

"***Cyber criminals won't be interested in my business…***" Wrong! Very wrong! Let me explain. Cyber criminals really could not care less if you make paperclips or jet aeroplanes. The method by which they identify targets is often completely indiscriminate. Like a lot of traditional crime – cyber criminals are mainly driven by greed and their motive is purely financial. Any business with an exposed Internet service such as a website or remote working capability must use an identifiable address for customers and / or clients to access it. This is identified by an Internet Protocol (IP) address – an online version of your physical address. It contains no obvious information about your company – it is just a sequence of numbers. However, cyber criminals can scan these addresses remotely to determine if there are any known vulnerabilities. And they will exploit any they find.

131.65.78.116

What happens in the real world?

The 2020 Hiscox Insurance Cyber Readiness report contains some disturbing statistics: 39% of firms in the UK reported a cyber-incident in 2019/2020 (down from 61% in 2018/2019). However, Gareth Wharton stated: '*While the number of firms reporting a breach is down, the cost and intensity of criminal activity in this area appear markedly higher. The numbers that have paid a ransom following a malware infection are chilling.* ***Nobody should doubt the scale of the problem***.'

Anecdotal information indicates that around 50% of small and medium businesses will go bust as a result of a breach. This is primarily due to the time and cost of getting the business back up and running, any fines issued by the Information Commissioner's Office (ICO) and the reputational damage that comes with losing data. Cyber-crime really can kill your business, so it is important to get it on your board agenda. Unfortunately, cyber-attacks have become so common that we rarely see anything in the media about it. These days, reporting is generally limited to huge corporations or government organisations.

What about local cyber-crime?

The CCU regularly deals with business-related cyber-attacks. Generally, these can be split into (1) Business e-mail compromise, (2) Ransomware and (3) Phishing. All will come with a financial implication – even if that is limited to the time taken to get back up and running. A number of these attacks could have been avoided had some basic measures been implemented.

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

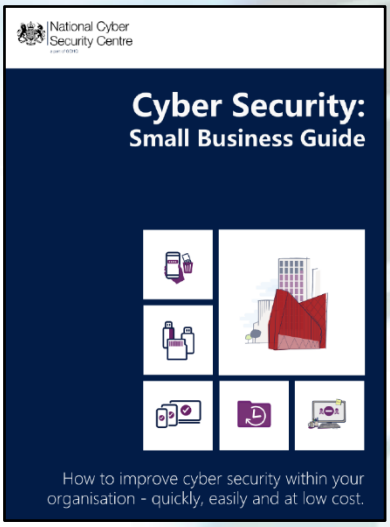
SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk

CYBER AWARE

south east
Regional Organised Crime Unit

How do I protect my business?

The world of cyber continues to get more and more complicated and it is often difficult to know where to begin. We recognise that small and medium businesses often do not have a dedicated team to manage cyber-security, but it is still important to understand and manage the risks.



Rest assured that some small changes can have a dramatic impact. Implementing basic measures such as using strong passwords, 2-factor-authentication, updating systems and being aware of phishing tactics would reduce the volume of crime investigated by the CCU by a huge percentage – and create less victims.

The National Cyber Security Centre (NCSC) has a wealth of information to support small and medium businesses. The Small Business Guide has been produced to help small businesses protect themselves from the most common cyber-attacks. It includes several topics including backups, protection from malware, keeping your mobile devices safe, passwords and protection from phishing. Many of these measures are low cost but will significantly reduce your vulnerability.

There are several other resources available on the NCSC website including a Response & Recovery guide which will assist you in preparing, identifying and resolving cyber related incidents. In addition, the NCSC's 'Exercise in a box' is a free online tool that allows organisations to test how they would respond to a cyber-attack.

What else can I do?

Planning for a cyber-attack is a great idea. Consider creating a Cyber Security Policy so that you and your staff know what their obligations are. Think about a Business Continuity Plan to enable a structured approach to be taken in the event of an attack. Educate your staff and make cyber security part of your everyday business considerations. Cyber Essentials is a great accreditation scheme to guard against the most common cyber threats and demonstrate your commitment to cyber security.

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

Where are all the resources you refer to?

General Information: https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations.

Small Business Guide: https://www.ncsc.gov.uk/collection/small-business-guide.

Response & Recovery: https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery.

Exercise in a Box: https://www.ncsc.gov.uk/information/exercise-in-a-box.

Cyber Essentials: https://www.cyberessentials.ncsc.gov.uk.

'There are 2 types of businesses – those who know they have suffered a cyber-attack and those who are yet to find out...'

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk