PARENT GUIDE

"When online you enter our world. We exist without nationality, skin colour, or religious bias. We are in control. This is our world now."

The **S**hadow **B**rokers

IT IS BELIEVED THAT :

The global cost of cyber crime will exceed $6 trillion annually by 2021, up from $3 trillion in 2015. This is the greatest transfer of economic wealth in history and will be more profitable than the global trade of all illegal drugs combined.

By 2019, a business will fall victim to ransomware (when data is illegally encrypted until a payment is made) every 14 seconds!

The Equifax breach in 2017 affected 145.5 million customers and is the largest publicly disclosed hack ever reported.

Meanwhile, the 'Wanna Cry' virus spread to over 150 countries worldwide and may have infected as many as 200,000 systems, crippling organisations from the NHS to Russia's second largest mobile operator MefgaFon.

There was a 600% increase in attacks against devices that are connected to the internet, from baby heart monitors and cardiac pacemakers to digital web cameras.

By 2025, there will be as many as 75 billion connected devices - many of which - are highly vulnerable; leaving a number of systems around the world at risk.

THE RISE OF TEENAGE CYBER CRIME

More and more teenagers, who are unlikely to be involved in 'traditional crimes', are becoming involved in cyber related offences.

"Offenders begin to participate in gaming cheat websites and 'modding' (game modification) forums and progress to criminal hacking forums without considering the consequences."

Recent studies have shown that financial gain - whilst a contributing factor - is not necessarily the real motivator behind increasing cybercrime. Rather the sense of achievement from being able to hack, coupled with the social prestige this brings appears to be the principle causes.

Many of these children - some as young as 12 - are academically gifted in science and technology and spend a large proportion of time sat on a computer.

"Parents and carers are frequently amazed to discover that they had been engaged in illegal activity because they spend so much time in their bedrooms"

THE COMPUTER MISUSE ACT

The Computer Misuse Act deals with cyber criminality. The terms are:

ACCESSING DATA WITHOUT PERMISSION:

For example, if you log into someone else's account
Or, you log into your own account but manage to access files or data that are not yours.
The maximum punishment here is 2 years and/or a fine that can't exceed £5,000.

ACCESSING DATA WITHOUT PERMISSION AND INTENDING TO DO SOMETHING BAD:

As above, however, this time you intend to do something bad, such as delete files or change what they say.

Alternatively, you might want to make the device’s software or even the hardware do something it shouldn’t.
The maximum punishment here is 5 years and/or a fine that can’t exceed £5,000.

DOING SOMETHING BAD INTENTIONALLY OR RECKLESSLY

Examples might include: planting malware; encrypting someone’s data, booting a friend of an online game or even obtaining someone else’s personal data for personal gain.
The maximum punishment here is 10 years and/or a fine that can’t exceed £5,000.

INTENTIONALLY OR ACCIDENTALLY CAUSING SERIOUS HARM

If you put lives at risk; cause injury, prevent the supply of fuel, food or water . . .

If you disrupt transport; affect national security or harm the economy . . .
It can be life - even if the harm done was accidental.

The law also prohibits you making; giving away, downloading or buying malware - even if you don’t use it!

WHAT’S ON YOUR CHILD’S COMPUTER

It is important to be able to spot the signs that your child is becoming involved in cyber criminality. The following hardware and software may indicate something is wrong:

Kali Linux:

A type of operating system (like Windows 10 or Mac OS) that is designed for penetration testing. It comes complete with a number of widely used hacking tools that are pre-installed for easy access.

Metasploit

Is usually found pre-installed with Kali but is often downloaded in its own right. It is best described as a collection of exploit tools that take advantage of system vulnerabilities and make hacking less technically demanding.

Virtual Box:

Most people run Windows or Mac OS on their home computer. However, by far the most popular operating system for hacking are Linux based. This means many ethical hackers use virtual software to run Kali Linux.

Think of virtual software as creating another computer on your existing one. This new machine can run any operating system.

Rubber Ducky

This piece of hacking kit comes disguised as a USB drive.

When plugged into a computer, the Rubber Ducky will load hundreds of dangerous hacking scripts at a rate of a 1000s words per minute. Scary stuff!

The Pineapple

The Pineapple looks like an ordinary Wi-Fi access point that you use at home to connect to the internet.

However, unlike its friendly namesake, the Pineapple comes with software which can help you to launch malicious ‘man-in-the-middle-attacks’.

In these types of attacks, the hacker inserts themselves between you and the internet. At which point, they can decrypt anything you send online on **any** digital device!

Tor

Tor is frequently misused web browser (such as Google Chrome, Opera or Edge) to grant access to the Dark Web - a place where you can purchase credit card numbers; drugs, hacking software or even, hacking services.

OPPORTUNITIES

Remember, the cyber security industry offers financially rewarding, technically challenging and prestigious opportunities for the right type of candidate.