PARENT

GUIDE

THE RISE OF CYBER CRIME

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

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

Other possible reasons could include, a lack of awareness of what actually constitutes cybercrime or how serious it is deemed by a society increasingly dependent upon its IT infrastructure.

However, the lack of credible academic research makes it exceptionally difficult to identify a typical 'teenage cyber criminal' or to even go as far as to say there is one!

Furthermore, no one seems to have any idea how much teenagers form part of these growing statistics. We hear that cybercrime is costing the UK '£27 Billion a year' but have very little idea how these whopping headlines break down on inspection.

WE NEED SECURITY SPECIALISTS

Indeed, there are very good reasons for young adults to be interested in cyber security - including the area of ethical hacking, which seeks to find weaknesses in security controls so that they might be properly mitigated.

Such work can, and often does, save companies thousands of pounds in damages and protects the sensitive data which we entrust them with everyday.

Technology has revolutionised every aspect of modern life. From cutting edge medical advances to the humdrum mechanics of industry & commerce.

The reliance on IT means that the security industry has blossomed. The opportunities to develop a deeply satisfying career that is financially lucrative is better than ever. It is no surprise, for instance, to find GCHQ offering lucrative bursaries and apprenticeship schemes for young teenagers with an interest in all things cyber.

TREADING A FINE LINE

Many parents, therefore, find themselves treading a fine line. There are a plethora of reasons to support a child's interest in security - including the world of hacking, but it needs to be done with some guidance.

WHAT YOU NEED TO KNOW

There are two key points here: A) What does the law say about cybercrime and B) How can my child learn about security safely?

THE COMPUTER MISUSE ACT

The Computer Misuse Act deals with cyber criminality and there are three key parts that we will paraphrase & discuss here:

UNAUTHORISED ACCESS:

If you log into someone else's electronic device or account or are accessing files & folders without that person's permission, you are most likely breaking the law. **The maximum punishment for this offence is 2 years and/or a fine up to £5,000.**

UNAUTHORISED ACCESS & IMPAIRING THE OPERATION OF A COMPUTER

Examples here might include planting malware, encrypting someone's data, booting a friend off an online game or exfiltrating data for personal gain. **The maximum punishment here is 10 years and/or a fine up to £5,000.**

CAUSING SERIOUS HARM

Finally, the harshest penalties are reserved for putting lives at risk; causing injury or preventing the supply of fuel, food, water and transport.

Don't forget, there are many IT systems where human welfare and safety are dependent - the NHS is a classic example. **The maximum penalty here can be a life sentence.**

BEFORE YOU BEGIN

Before learning to hack, you child needs to understand the Computer Misuse Act and why hacking can have devastating effects for victims when not done ethically and without serious consideration. Nor are you protected from prosecution by claiming ignorance of the law.

LEARNING TO HACK SAFELY

There are a lot of tools that can support the development of a child wishing to hack.

KALI LINUX:

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

Installing Kali Linux can be a challenge - especially if you don't want to replace your existing operating system. For this reason, many hackers install VM Ware first.

VIRTUAL MACHINES (VMWARE):

If you install VM software, your computer - and all the things on it - works as it always has. However, when you fire up your newly installed VM ware, you can add and use other 'computers'. A MacBook could - in effect - have a Windows computer on it and a Linux system too.

Be warned, when you run two systems on one computer, you affect its performance. However, the benefit of a VM is the ability to reset everything using 'snapshots' when things go wrong - and they inevitably do.

METASPLOITABLE & OTHERS

Metaspoloitable is an intentionally vulnerable Linux virtual machine that can be used to test security tools and practice common penetration techniques without the fear of doing harm to others.

Online equivalents also exist. For example; hack.me, HackThis and Immersive Labs are certainly growing in popularity. Many others sites can also be found with a little thought and patience using your favourite search engine.

PAID FOR AND FREE COURSES

It is amazing how much some teenagers can teach themselves by pillaging free online resources and videos posted on YouTube. However, for many it is much easier and more effective to pay for an online course.

These courses are often produced by security professionals and include comprehensive video tutorials. Indeed, with a bit of research you can not only find these courses but also how well people rate them. Good sources include places like Udemy and Lynda.com.

OTHER TOOLS

There are other hacking tools that are proving popular with young adults.

Key grabbers - a discreet plug-in that records what you type as well as USBs loaded with malware (such as the Rubber Ducky & Bash Bunny) are both worth knowing about. Just as popular are devices like the Pineapple WiFi. These target free WiFi connections and allow the penetration tester to view an individual's online activity.

However, before rushing off to purchase such equipment, a serious conversation needs to occur about how they should and should not be used. Not only is it critically important to have the permission of the intended target but time and effort must be spent making sure that innocent parties are not affected by your actions.

TOR

Finally, we come to Tor. Tor is a browser, just like Internet Explorer, Edge, Chrome or FireFox. It also acts like a VPN, hiding your online activity and protecting your identity from others.

Tor has many legitimate uses but controversially is also associated with the Dark Web. Here, teenagers can purchase hacking tools as well as drugs, weapons and credit card information. Before allowing any minor to download Tor, you must be completely satisfied that it will be used safely and appropriately.