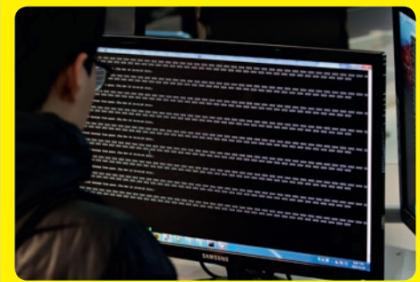


The shady world of cyber hacking

As technology advances, find out how to stay safe online

The online world can seem like an exciting place. You can play games, shop and chat with your friends at the click of a mouse or the swipe of a touchscreen. But there are also lots of hidden dangers. A new Government report released last week revealed that more than two thirds of British businesses have experienced some form of cyber attack in the past year. The attackers used spyware – computer software that can access private information like passwords. They also infected computers with viruses, simple programs that cause nuisance or damage to a computer. The survey was conducted after the phone provider TalkTalk was hacked last year. Hackers stole bank details and personal information from more than four million customers, which hackers could use to steal people's money. The Government is now investing £1.9 billion over the next five years to tackle cyber crime.

What is cyber hacking?



Cyber hacking is when someone breaks codes or passwords on a computer to gain access to a person or company's private information without their permission. The hacker can see personal information, such as bank details, or send messages pretending to be someone else. Hackers use all sorts of tricks to do this. They might use a program that makes sequences out of all the letters in the alphabet to guess someone's password. Or they will send an email with an attachment or a link in it that might seem really tempting to click. If a person clicks open the attachment, software is automatically downloaded to their computer, which allows the hacker to break into the computer.

Is hacking always bad?



There are lots of reasons why people hack into computers; not all are bad. However, hacking can be illegal and result in long prison sentences. In the UK, hacking is an offence under the Computer Misuse Act (1990). The law says it is an offence to access someone else's files without permission, and to alter computer data without permission, such as writing a virus to destroy a person's data. There are different categories that hackers fall into. Bad hackers are sometimes called "black hats". They hack into personal or company computers to steal private information. They might use the information for their own gain or post it online because they think it is right to reveal information, sometimes about companies and governments to the world. These activities are criminal offences. Other hackers are sometimes known as "white hats". They will deliberately break into the security

system of a company to let the company know that their security protection is weak. Some companies end up giving these hackers jobs. This type of hacking isn't usually illegal. There is another group, so-called called "grey hats". Grey hats sell the information they find about security leaks to government agencies. They are known as grey hats because even though they are selling to people who they think will use the information for good, this is not always the case. Some agencies use the information to spy on people.

If you have been a victim of hacking or cyber bullying make sure you talk to an adult you trust. For more information or help about cyber bullying go to cybersmile.org/



Five famous hackers



1 Steve Wozniak
You may know him better as the co-founder of the tech company, Apple, but did you know that in his teenage years Wozniak was a playful hacker? Wozniak has spoken about how he used to hack into his friends' and family's computers for fun. He once left nine pages of Polish jokes that would pop up on screen when they opened their computers. He described his hacking as "white-hat hacking" because it was never for the purpose of stealing.



2 Anonymous
Anonymous is an international group of hackers who believe in freedom of speech. Since 2008, the hackers have broken into the accounts of people they don't like, such as the US presidential hopeful Donald Trump. They have also taken down Twitter accounts related to terrorists. They sometimes use distributed denial of service (DDoS) attacks. These work by overloading websites with traffic, which means entire websites can be knocked offline.



3 Kevin Mitnick
Mitnick has been described by the US Department of Justice as "the most wanted computer criminal in United States history". He has hacked into some of the biggest technology and telecommunications companies in the world, such as Nokia and Motorola. He also stole computer passwords and read confidential emails. In 1995 he was jailed for five years. Now he runs a company that helps test the strength of other companies' security.



4 James Kosta
At the age of 13 James Kosta was already earning £1,000 a month as an IT consultant. A year later he started hacking the sites of big businesses and the US military. He was caught by the FBI, the US security service, and sentenced to 45 years in jail for his crimes. Instead of sending him to jail, the judge offered him a job as an intelligence analyst, at the age of 18. He then joined the CIA (the US foreign intelligence agency) a few years later.



5 Julian Assange
Assange has hacked into the US Department of Defence and NASA. In 2006 Assange, along with others, went on to create WikiLeaks, an organisation that publishes confidential information to the public. To escape arrest in the US for leaking documents about US officials, Assange requested political asylum from the Ecuadorian embassy in London where he has been living since 2012. If he leaves the embassy he will be arrested.

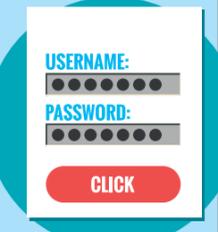
DID YOU KNOW?
Anonymous are known for their black-and-white Guy Fawkes masks, to hide their faces in public and online. Guy Fawkes tried to blow up the House of Parliament in 1605. In the 1980s, graphic novelists Alan Moore and David Lloyd created a comic strip, "V for Vendetta". The main character wears a Fawkes mask while battling against an oppressive government.

Staying safe online

It is important that you protect yourself online from people who might want to steal your private information. Here are a few tips to stay safe:

Protect your passwords

Never use a password that people can easily guess, like your family pet's name. Change your password so it has a mixture of letters and numbers.



Always log off

If you're using a public computer always make sure you log off before you leave. That way the next person can't access your emails or social media.



Don't open junk mail

Don't download attachments from senders you don't know; it could be a hacker trying to gain access to your computer. Only open emails from senders you recognise.



MINI HACKERS

Facebook is asking hundreds of schoolchildren to play a hacking game, because it is worried about its cyber security. The game, Facebook Capture the Flag, is similar to the board game Risk. It asks players to hack a website in order to conquer territory. Facebook is offering cash rewards to people who find faults in the web code while playing the game.

