CYBER CRIME
STAY SAFE!

PRESTIGE LOGIC

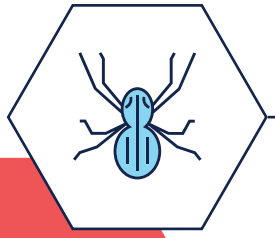
CYBER CRIME **STAY SAFE!**

If someone asked you to take a wild guess at the UK's biggest crime, what would you think? Burglary maybe? Common assault? Or perhaps you might take a more humorous approach and suggest man buns or women with ridiculous eyebrows?

Well, you might be surprised (and a little concerned) to find out that the most commonly reported crime in the UK right now is actually online fraud, AKA cyber crime.

With one in ten people now falling prey to internet fraudsters and over 5 million cases reported every year, cyber criminals are very real predators that can have a devastating effect on lives and businesses. And these figures are just the tip of the iceberg - many more cyber crimes are believed to go unreported because victims feel too embarrassed to let on that they've been duped by a stranger sitting behind a keyboard.

The digital age comes with lots of well documented pros and cons. We can now work from anywhere in the world and stay constantly connected, but that has a knock on effect on our personal lives and stress levels. We can find out anything we want about any subject, but we're suffering from sensory overload and our libraries and book shops are suffering. And, now we no longer have to keep millions of trees worth of paper files in dusty cabinets, keeping personal data online puts us at risk.



CYBER THREAT IS THE **BIGGEST THREAT** TO SMALL BUSINESSES

During 2016 alone, cyber crime cost businesses £29 billion. That's an obscene amount of money by anyone's standards, and the really scary thing is that the ever increasing industry called data theft is now relatively easy for anyone to get involved in. Gone are the days of 1980s sci fi movies, where computer hackers were dark, mysterious and possessed savant-like levels of intelligence. Today anyone with the inclination and £50 to spend can pick up a fairly powerful piece of software that will enable them to hack into computer systems and wreak havoc.

The aptly named Wannacry attack on the NHS in May 2017 sent shockwaves across the world - one of the largest and most important organisations in the UK was brought to a standstill by a bunch of hackers. A form of malicious software known as a ransomware cryptoworm; Wannacry targeted computers running on MS Windows, encrypting their data and demanding ransom payments for their safe return. Within just 24 hours it had infected more than 2 million computers, many of which belonged to the NHS. The loss of data left the organisation with no other option than to offer emergency-only services until the attack was stopped.

HACKERS ARE **EVERYWHERE**

From online shopping fraud to malevolent viruses, we're at the mercy of dangerous keyboard warriors with dangerous software at their fingertips. More than half of the internet crimes committed each year come from abroad, and they'll often make a beeline for smaller businesses without IT departments. These hackers are quick, smart and opportunistic, and with new threats appearing almost every day it's impossible for even the most skilled software designers to keep them out.

Even with all these new threats popping up all over the place, many of us take a somewhat laid back approach to looking after our internet security. To busy people, waiting for a PC to update the latest version of anti-virus software means missing out on valuable business time - so the temptation to just click on the "remind me later" button is often too strong to resist. Trouble is, by the time you've clicked on that even once, a hacker could have gone in and stolen all your valuable data. Waiting ten minutes for an update doesn't sound so bad now, does it?

Exploit kits

These are easy to pick up when you know how, and since they're thought to be responsible for the vast majority malware infections throughout the entire world, they're pretty deadly too. These kits are distributed both publicly and on the black market and appeal to both hardened cyber criminals and newbies. They work on web servers, looking out for weaknesses and then running malicious code which enables the hacker to have complete control of the system. These destructive little kits can be purchased for as little as £50 but are capable of causing millions of pounds worth of damage.

Most common types of cyber scam

As we said earlier, cyber crime is constantly evolving so it's impossible to provide a conclusive list of all the threats in one short guide. By the time you've finished reading this someone will probably have already thought of a new way to hack into a computer network and cause chaos - but what we can do is take a quick look at some of the most common forms of attack.

Crypto attacks

These prey on the uneducated by sending emails with attachments claiming to have come from a trusted source. They look like the real thing, but once you open the attachment malware will automatically be installed on your PC. Once it's on there, the hacker will take total control of your data over a period of time - long enough so that nobody notices it's happening until it's too late. Using a key logger, they'll be able to watch everything you're doing online, meaning credit card details, personal logins and sensitive information can all be stolen. They then present the unsuspecting user with an on-screen ransom note: Pay up or say goodbye to your data.

Phishing attacks

This is when groups of cyber criminals work together to steal your data and sell it on. Often finding their way onto your network through users connecting on bad links, they'll steal your client data and send them emails pretending to be from you. They also commonly steal credit card information and bank details which are sold onto other cyber thieves who use your data for identity theft scams. Get caught up in a phishing scam and it will cost you time, money and probably the reputation of your business.

Malware

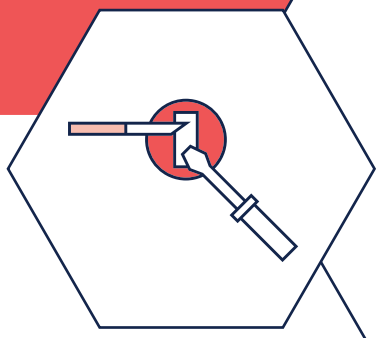
Specially created to cause mayhem, this is one of the nastiest forms of cyber crime out there. It's often used by unscrupulous businesses who want to steal their competitors' client data or simply send them spiraling into organisational chaos. They use fake advertising - AKA "malvertising" - to create interest, leading naïve users to click on dodgy links (do you see there's a theme here?!).

You may think you're too smart to get caught out by something like this, but don't be too sure - often these fake ads look so much like the real thing that even the most savvy internet user can get caught out. Before you know it, malicious code is all over your PC and spreading like wildfire through your organisation.

There is **good news**

Despite all this misery and foreboding, it's not all doom and gloom. It is entirely possible to keep your business and its people safe from cyber criminals; it just takes a combination of two important elements - prevention and fixing.

So, let's take a look at them, and their components, one at a time.



Preventing cyber crime

We all know the old adage "prevention is better than cure", and when it comes to IT security this is particularly true. Depending on the type of cyber crime you fall victim to, once your data's gone it could be impossible to retrieve. Just imagine all your important work and contact information, gone. If you've only saved it in one place, you're doomed. **That brings us to the first part of the prevention process:**

Prevention process part 1 **back ups**

Anyone who's ever spent ages working on a document and failed to save it will understand this one. Whilst most computers do regular back-ups, you should never take it for granted. If you want to up your security you need to make sure that you have stuff saved in more than one safe place, so don't get caught out.

Prevention process part 2 **awareness**

According to a 2014 report from IBM, a whopping 95% of online security problems involve human error. Important files left on trains, mobile phones lost, USB sticks shared, malicious email links innocently clicked on. The key here is clearly staff training and awareness so people understand their personal responsibilities in terms of security. Write clear policies, organise regular training sessions and be sure everyone is kept up to date.

Prevention process part 3 **technology**

If you want to keep the bad guys locked out, you'll need an arsenal of anti virus software, and the more you have, the better protected you'll be. A multi layered security system including components like identity based access, vulnerability assessments, intrusion detection, network control and firewalls works best. Make sure everything is up to date and run regular updates - **DON'T IGNORE THEM!**

Fixing your **business** after a cyber crime

Depending on its severity, the data loss resulting from cyber crime can be fixable. That said, it takes the average small business user around 200 days to even notice a data breach has taken place so don't be surprised if damage has been done.

The important thing is to act as soon as you realise something bad has happened and identify the source as quickly as you can. Once you've got more information about the kind of attack, what caused it and how much data is affected, your IT support company should be able to spring into action.

Lost files should be re-installed, infected ones should be removed, new security patches should be applied and all logins should be re-set. All sensitive data should be separated and backed up. You'll also need to notify affected customers straight away - this isn't an easy job and can easily cause clients to go into meltdown if not handled delicately by whoever's in charge of PR.

Now's also the time to have someone undertake a full risk assessment and virus scan and identify any other potential threats before they happen.

Again, if your data is backed up, you'll find yourself in a much more favourable position than you will if you're unprepared - **so BACK IT UP!**

Ultimately, the security if the data in your organisation is up to you. It's not Microsoft's fault if a hacker finds a way to get into your files, it's yours. Sorry if that sounds harsh but it's true. Think of it this way - if you go out all day and leave all your doors and windows open, can you really complain if you get burgled? Of course it's the burglar in the wrong; they're the criminal here, but did you play a role in letting it happen? Well, sadly yes.

It's the same thing with your cyber security. If you know your anti-virus software has run out or needs an update but you choose to leave it until later, you're leaving your doors wide open and making it much easier for hackers to do their thing. But if you lock the doors, set up cameras and have a really scary looking guard dog move in they're more likely to think twice and move onto the next unsuspecting victim.

The **bottom line**

cyber crime is happening right now and if you're not careful you could become one of the countless businesses who fall victim. Be prepared, act fast and don't be complacent.

PRESTIGE LOGIC