How to Avoid Becoming a Victim of Cyber Crime

By Richard Plumb, Designing Out Crime Officer, West Midlands Police

Cybercrime is a problem for everyone. Regardless of whether you own a computer or not, the people, businesses and organisations that hold your data do so in a digital format and they keep your data in digital records. Even before the computer age however, businesses have always held your personal information and that information has always been at risk of being lost. Whether it's an employee leaving important documents on a train or a thief breaking into a building and stealing them; information security is certainly not a new concept.

The difference between information security in the present day and information security of time gone by, is simply about speed and distance. Computers allow for businesses to access your data quicker and more efficiently than ever. This in turn, allows us as customers to do fantastically clever things, like seeing who's ringing your doorbell from the Bahamas or paying for petrol even when you've forgotten your wallet! Unfortunately, this ease of access also allows for criminals to operate in equally clever ways and we need to be careful not to leave our digital back door open.

So, what can we do to make sure we're safe? Well the National Cyber Security Centre (NCSC – www.ncsc.gov.uk) are the government body created specifically to give guidance on the subject of cyber security. In addition to the NCSC, other not-for-profit organisations have been set up to give advice too such as Get Safe Online (www.getsafeonline.org).

As a crime prevention officer with specialist knowledge in this area, I try to take the advice from websites such as the ones above and tailor it suit our communities.

Here are some of my top tips to keeping yourself safe online:

- Choose strong passwords.

  A strong password is one that is long, memorable but not easy to guess. Make it personal but not obvious so that others might know it. Try to picture a memorable moment in your life and use three random words from that scene. For example:

  "When my first child was born I remember everything about that moment. I'll never forget when the nurse handed her to me for the first time. Picking three words from that scene, my password will be "HospitalCurtainsPink", because I remember the curtains around the hospital bed were pink. I could make it stronger by adding the date on the end and even a special character or two."

- Treat all unsolicited emails with caution and never click on links to visit unknown web sites.

  This is the most important tip of all! Never click links in unsolicited emails. If a website has emailed you to say your account needs urgent attention, it might be genuine, but it also might be fake! Delete the email and go to the website through Google or through your browser's URL bar. Don't use the link in the email or you could be handing an attacker your password on a plate.

- Don't open attachments in emails that you're not expecting.

Attachments in emails could be dangerous and could even completely destroy your computer. Make sure ALL attachments are scanned by your anti-virus software and if you're not expecting the email, do you really need to open it? Remember, curiosity killed the cat.

- Update software and apps regularly.

  When your computer or phone says it needs to update, it's normally because there are problems with the software that need fixing. These problems are like open windows to a possible cyber criminal. Keep your digital doors and windows locked by ensuring all software is current and up to date.

- Install anti-virus security software and make sure you run regular updates

  Your anti-virus software needs to update too. Anti-virus can only stop attacks that it knows about, therefore keeping it up to date ensures it knows how to stop all the latest attacks and gives you peace of mind that your computer is working to keep itself safe.

- Review bank and credit card statements regularly.

  Let's be honest, we don't do this enough. I'm certainly guilty of that too, but if you're going to identify if you've been a victim of cybercrime, you need to check your bank statements. If you see regular payments that you don't recognise, query them. Your bank can give you more information and most will also help you to better protect yourself if you have been a victim of cyber crime.

- Finally, report all cyber crime to Action Fraud.

  Action Fraud are the national reporting agency for all cyber crime offences. We need information about cyber crime so that we can work out how best to police it. Don't let cyber criminals get away with it.

You can report all cyber crime to Action Fraud on 0300 123 20 40 or by visiting the Action Fraud website here: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

Richard Plumb

Designing Out Crime Officer

West Midlands Police