CYBERMAN365

ESSENTIAL STEPS TO AVOID BECOMING A CYBERCRIME VICTIM

Cyber-crime against private individuals and families is rapidly becoming a new growth area in the US. For example, the FBI reported that cyber-crime in 2019 had affected almost 470,000 complainants with suspected losses in excess of $3.5 billion, roughly $7,000+ per complainant.

This is why, Neil Gurnhill, CEO, of Node International, a leading cyber underwriter at Lloyds of London has launched an innovative insurance product, CYBERMAN365[1], and why Neil is sharing his expertise of coping with cyber-crime.[2]

OVERVIEW

The three most common cyber-crime threats are:

Gaining access to banking details and suffering financial loss

Identity theft that then leads to financial loss, taking out loans, credit reference damage, etc

Loss of computer data files through ransomware attacks

How can you prevent these threats from happening?

WHAT CAN YOU DO?

Just like protecting your family and home from criminals, you must be very watchful at all times and this watchfulness has to become a habitual behaviour.

At home, you may notice suspicious activities in your street, ensure your doors are locked, have the best physical security you can afford and discuss security with all your family, whatever their age.

Conversations such as keeping valuables out of sight, insuring your contents and valuables, never talking to strangers as a child and to be wary of people you don't know as an adult. These are all valid discussions that make us aware of these physical dangers and actively avoid them.

You have to do the same for cyber-crime. If you don't try and prevent and protect now, you will become a victim of cyber-crime and increasingly so.

WHAT ARE THE MUSTS OF PREVENTION AND PROTECTION?

Below, I will highlight the safeguards you MUST have:

Security software that is up to date and the best you can afford
Too many individuals and families:

- Use old security software,
- Don't switch on automatic updating to ensure security patches are always current,
- Have out of date internet browsers,
- Don't automatically back-up their files every 15 minutes,
- Don't use a VPN (virtual private network), so they're visible to criminals when using the internet.

Stand back, reflect and re-organise. Talk to the tech-savvies you know at reputable stores, local security consultants, your tech department at work and Google 'the best security systems' and get the best advice you can.

I use Bit Defender Total Security (which contains a VPN) which automatically updates.
I update my computer system and files to the Cloud every 15 minutes using Acronis True Image.
If you need to, download the latest operating systems and update your devices.

Sort out your password habits
White hat hackers or ethical hackers are demonstrating every day just how easy it is to crack personal passwords and the FBI reports that Email Account Compromise is one of the rising crimes because personal passwords are very easy to crack or hack into. If your password habits are ineffective, it is time to reflect and change your habits.

There are two basic bad habits:

- First, most people tend to use very simple passwords, ones that are easy to remember and then they may also recycle them across multiple accounts. A hacker can break these in minutes and they start by looking at your Facebook page for hints.

- Second, irrespective of whether a password is hard to crack, many don't change their passwords regularly. For example, they have a great password for their bank accounts but it never changes from month to month.

So, the tips are:

- Use a password manager from a reputable security company. This creates strong and unique passwords for every account.
- Aim for 10 to 12 collections of keyboard numbers, symbols, upper-case and lower-case characters, something like this: Adk@?)3981+BjHP and change them regularly. Use a unique combination for every account.

Develop the good habit of NOT clicking on links
The vast majority of cyber-crimes start with one very simple mistake – clicking on links too quickly. These links may be on websites, Google search websites, emails, email attachments, spam emails, clickbait photos, official-looking forms, free games and more (the list is endless!).

Phishing links are sent out in their thousands every minute of the day by automated bots, (networks of highjacked computers). Criminals send these out for one purpose only, to trick you into clicking on the link.

The consequences are high, the result may be accidentally installing a piece of malware that logs your keyboard strokes to get passwords and then reports back to the criminal. Or, it could be the start of a ransomware attack. Or, the beginning of an identity theft process.

Fortunately, good security software protects you – but some get through. We all have to change a bad habit of trusting links.

Question each link you find by considering the following:

- Do you know who it's from?
- Do I trust this person?
- Should I check that it's really from the person they claim to be?
- Is the website authentic?
- Is the URL in the taskbar spelt correctly?

Regularly asking these questions will make avoiding phishing second nature.

Wherever you can use two-factor authentication when you are transferring money
All banks use this and it is safe. Unfortunately, criminals have now found a way to intercept the second code so it transfers to their own bank account. Be very wary.

Be very wary of giving anybody access to your personal information or devices
Common financial scams:
- Your bank may ring you and ask for your password, as a security measure.
- A security expert rings about a security flaw on your computer.
- A so-called computer imitates a local store and is willing to fix a problem.
- An officer from the IRS rings you to announce a tax rebate.

To avoid becoming a victim, put the phone down and ring the number you know is correct to check that your caller is authentic.

SUMMARY

I hope this article gives a useful view of the safeguards you need to use for the evolving cyber-risks you will face in 2020 and beyond.

If I were to select the three most important safeguards, it would be these:

- Use the best security software you can afford
- Sort out your password habits
- The most important, be very wary what you click on

These three apply to everyone. However, if you are young (from pre-school to College), elderly and feel vulnerable, wealthy, not familiar with computing then they are especially important.

SOURCES

1 Cyberman365 offers two services, allowing our clients to create their own unique personal cyber insurance. Cyberman365 IDNotify is Identity Theft Insurance combined with extensive digital monitoring and instant alerts. Cyberman365 HomeSafe is an innovative Home 'Internet of Things' protection allowing users to secure their home, network and devices from cyber attacks. Both services are backed by insurance and incident response. www.cyberman365.com

2 Neil Gurnhill is the CEO of Node International, a specialist, cyber-insurance underwriters at Lloyds of London. Neil is regarded as an international expert in all matters affecting cyber-security and insurance and his company, Node International was founded to provide cyber-insurances services to US corporate and individuals. Node International, since 2019, is now part of the insurance group H.W.Kaufman of the US. Node provides its services throughout the US, UK and the EU.