The Internet & Cybercrime

by Helen Murphy

Without a shadow of doubt, we can probably all agree that the Internet has been and continues to be a revolutionary instrument. It provides us with access to massive amounts of information at the click of a button, opens markets to us that heretofore were unreachable and allows us to witness global events in real time rather than hearing about them hours or days later.

Whilst the internet was originally designed as a way for government researchers to share information, it was opened to the public in 1991 with the invention of the World Wide Web. In 1993-1994, websites for everyday use became available. Whilst its adoption in everyday use was slow because computers were seen as a business device rather than a personal tool, once mainstream adoption of this new technology achieved critical mass, the use of the internet increased exponentially.

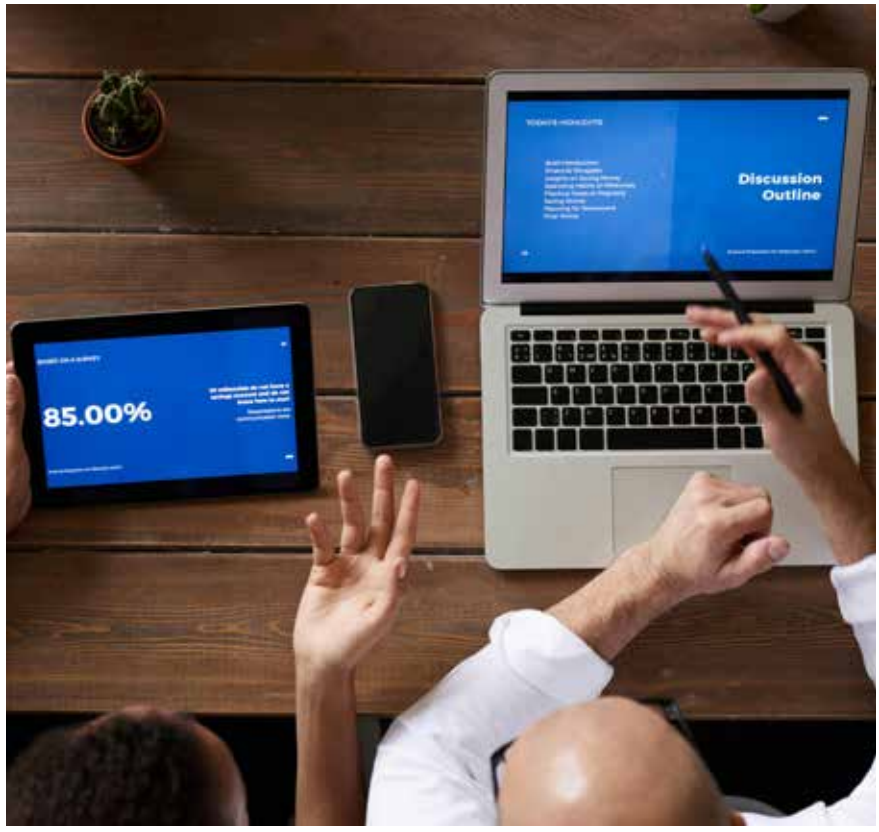
Mobile devices have turbocharged this usage as now we carry the internet with us in our pockets or purses 24 hours a day, 365 days a year.

The development of the Internet of Things and AI will further increase our reliance on the internet.

Whilst most internet related things are positive, unfortunately there are plenty of actors out there who use the internet and our naivety to impose harm and financial loss.

Some of these attempts to catch us out are now so recognisable that we instantly dismiss them – the various Crown Princes from countries all over the world who email us asking for our support as they are having a hard time financially now. The millions in Euro/Dollars/Sterling that are sitting in the bank accounts of deceased individuals who have no heirs remain in those bank accounts. The winnings from lotto draws that you didn't even realise that you had entered are still waiting to be claimed.

You may still get these phishing emails but we probably all recognise them for what they are.



However, as technology becomes smarter, so do the people trying to catch out the uninitiated or careless.

We have all read the stories about companies receiving emails from a supplier advising of a change of bank details and while we may think that this only happens to smaller, less informed companies, consider this:

"Using imitation email addresses, Lituanian national Evaldas Rimasauskas successfully defrauded US tech giants Facebook and Google out of a total $122 Million Dollars. Rimasauskas did this by sending fake invoices that were disguised as coming from a common supplier, Quanta Computer Inc, based in Thailand.

This demonstrates that even the largest corporations can be conned by a committed fraudster."

Mr. Rimasauskas was sentenced to 5 years in jail in 2019.

Facebook and Google are far from being naive when it comes to the internet and yet, they were caught out by a "simple" invoice scam.

Unfortunately, the people operating in the darker regions of the internet are becoming more and more sophisticated in their "art" and are receiving greater financial support from nefarious State actors and because we as individuals and businesses are storing more and more information in digital form in

the Cloud, the opportunities for these people to wreak havoc is growing all the time.

Whilst losing money on an individual basis – such as the cases that are reported in the paper from time to time – is painful, it is probably the hit to our confidence that is the worst thing. It's the "how can I have been so stupid" question that goes round and round in our heads for days and weeks after. We berate ourselves for having fallen for the scam. We wonder would anyone else have known it was a scam. Our internal reputation, i.e. our ego, takes a hit.

Now, imagine that it wasn't you individually who was the victim of an internet hack. Imagine instead that it's your company and hackers have gained access to your files including the personal and financial details. Or imagine that hackers have taken control of your computer systems, and you are locked out of those same files.

Your first port of call in the event of this happening is going to be your IT support department. If you're company is big enough to have a department like this then work on rectifying the situation can start immediately – even though the outcome may still be unpleasant.

If you are too small to have a dedicated IT department, you are on the phone to your IT support provider, hoping that they can bring you back from the brink.

After those calls, who's next? Your regulator will need a call to inform them of the situation and probably the Data Protection Commissioner.

But who's going to ring your clients to inform them of the issue and how do you evaluate the potential reputational damage that such an event will create?

"Hi Ms. Client, listen, our systems have been hacked and we're not sure, but your financial information may be in the hands of the hackers. Our IT team are on the case, but we don't know when we will regain control of our systems. It's probably a good idea to change passwords on your bank accounts etc."

Do you need to employ a PR company to smooth things over?

How are these costs as well as the increased spend as IT try to retrieve the situation being covered?

This is where Cyber Security Insurance can help. Cyber Security Insurance can pay for professional support to help businesses restore data and be up and running as soon as possible.

It can:

- Offer protection from cyber risks which could be damaging to a business and its reputation.
- Assist in helping business recover after a cyber-attack.
- Pay for professional support to help businesses who are the victims of cyber-crime.

It is not a prevention, but it helps protect against a financial loss.

Whilst Cyber Security Insurance can help alleviate the costs after an event has occurred, it is always better for the event never to have occurred in the first place. Unfortunately, too many of us still use the same password on multiple applications.

Passwords should ideally be between 8 and 64 characters long and whilst the thought of remembering a 64-character password may be daunting, using a password that is also a sentence may be easier to recall.

The above sentence is 64 characters (without the full stop). The length of this password makes it extremely difficult to crack.

Don't share passwords with colleagues.

Computer systems should have strong anti-virus protection. Digital Data should be encrypted. Use Firewalls.

Use up to date software and make sure to apply any patches or fixes issued by the provider.

Use Multi Factor Authentication. When you log onto an application, your phone receives a code which needs to be entered as well to confirm that it is you logging in.

However, no matter how good the security on our systems is, there is always the human factor which can breach the strongest defence.

I will leave you with this story as an example.

A colleague of mine received a call from his father asking if he had sent an email with a virus to him. My colleague had no clue what his father was speaking about but asked his wife if she had seen any strange emails. "Oh yes" she replies. "I saw an email come in with the title 'Had a great time last night, can't wait to do it again". "And what did you do?" asked my colleague. "Oh, I clicked on it" she replied, "but nothing happened, so I clicked on it another 20 times to try and open it".

My colleague had to explain that this email contained a virus that sent itself to all the email addresses on his computer because of her attempting to open the original email in the first place.

Unfortunately, the best IT practices and security in the world is easily defeated by a spouse who thinks her husband is up to something nefarious!

Whilst this anecdote may bring a smile to all our faces, it highlights the fact that the weakest link in any cyber security is always the person at the end of the keyboard.

Here in JDM Insurances, we would be delighted to discuss Cyber Security Insurance as an additional layer of protection for your business. Please do not hesitate to contact us for further information.

Helen Murphy

Managing Director, JDM Insurance Services Ltd