FINANCE UPDATES

JULY 2020

CAMPBELL & McCONNACHIE

chartered financial planners

PROTECTING YOUR CASH FROM CYBER THREATS

How safe is your wealth in the current climate?

While the UK tries to deal with the economic impacts from COVID-19, reports are rife of fraudsters stepping up their attempts to access your money.

Since the outbreak of COVID-19, around three in five scams are bank-related, followed by insurance (35%) and pensions (19%).

Worryingly, one in five adults in the UK has either been a victim of a pension scam, or know someone who has. When you step back and think about the research, conducted by Opinium, it could equate to around 5.2 million retirement savers in the UK.

Business owners are also targets for cyber attacks, while online scams are estimated to cost around £670m a year in lost cash.

Understandably at this nervy time, both for people's health and the economy, protecting your wealth is a key priority. Hopefully this article allays any fears you may have.

IS ONLINE BANKING SAFE?

Despite the research suggesting wealth held in banks or building societies is the main target, those are some of the safest organisations in the world.

They work with regulators to help ensure:

- your money is kept where it should be
- your data stays the way it should
- fraud is prevented, although this is a difficult task
- banking services are kept up and running.

The Financial Conduct Authority (FCA) usually requires your bank to refund any unauthorised payments from your account.

Your bank must refund the unauthorised payment without delay, usually within 24 hours of being made aware of the problem.

The bank cannot claim the use of your online banking password, card or PIN number proves you authorised a purchase.

If it can prove you were at fault, by demonstrating how you failed to protect sensitive information, you will not get a refund.

When you receive a debit or credit card, or sign up for online, mobile or phone banking, your bank will advise how to stay safe.

Fraudsters have been known to send phishing emails containing a link to a fake bank website, asking you to update your account or security details. In such cases, always phone your bank to check the authenticity of these suspicious emails before giving away any confidential information.

ARE MY PENSIONS SECURE?

Newspaper headlines often involve stories of people who've 'lost their pensions', and it is easy to imagine this is quite common.

In reality, most people receive their pensions as expected and without any problems, but this doesn't make for a good story.

While it's rare for people to lose their pension, or get less than expected, if things go wrong, it's good to know there is protection in place for your pot.

In most cases, especially where you have received independent financial advice, your pensions will be secure.

Usually when things go wrong with pensions, it's down to people investing their money without advice and making poor decisions.

Just last month, the FCA said that do-it-yourself savers who are going online to search for investments are prime targets for fraudsters.

Typically, fake websites look official and ask the target to provide personal or financial information, for example, to update existing information.

Naturally, an economic downturn presents opportunities for investors who are comfortable with a high level of risk to seek big returns on investments.

Although some scams offer tell-tale high returns that seem too good to be true to tempt you into investing, they may also offer realistic returns to make their product seem legitimate.

Those offering or promoting investment opportunities or products of the type typically found through Google are not necessarily authorised or regulated by the FCA.

They almost always involve high charges and offer very little protection if things go wrong, so always seek expert advice.

ARE BUSINESSES VULNERABLE?

Within 24 hours of the furlough scheme going live, fraudsters sent a flurry of phishing emails to unsuspecting businesses.

These emails claimed to be from Jim Harra, chief executive at HMRC, and attempted to get hold of bank details for the supposed payment of funds.

Criminals are also bombarding business owners with calls and texts, which impersonate a range of organisations, to trick them into providing personal or financial information or money.

Businesses can follow three simple steps to stay safe online:

- keep strong, unique passwords for all of your online accounts
- protect all your devices with up-to-date anti-virus software
- ensure all of your software and operating systems are up-to-date to reduce any weaknesses.

Most modern-day businesses in the UK are heavily reliant on a computer system or use online software to hold a huge amount of electronic data about customers, employees or anything else.

There are, however, measures you can put in place to protect your business from online threats, and **cyber insurance** can offer you a safety net should the worst happen.

Cyber insurance

Most businesses rely on information technology to some degree, and with it comes the risks of business interruption, income loss, damage management and repair.

A good cyber insurance policy will include compensation for any financial loss incurred as a result of a cyber attack which disrupts your business. This could include the costs involved with restoring any lost data, investigating the breach, and cover for IT services to get your business up and running.

Cyber security breaches can be followed by fines relating to lost customer or client data, especially with the new data protection regulations (GDPR) that came into force in 2018. Cyber insurance may cover any financial liability.

There are policies out there which contribute towards the costs of installing a new or upgraded online security system, as a further preventative measure.

Cyber insurance can also provide cover for incidents relating to your business's data and computer systems that aren't as a result of a malicious cyber-attack. For example, if your IT system fails because of a power cut or natural disaster, your policy may cover the costs of repair and restoration.

Criteria

Insurers may ask you to meet certain criteria before they give the green light for your business to take out cyber insurance.

Most commonly, insurers ask for a threat assessment to ascertain where your business is vulnerable online and what you may need to claim for.

You may also need to show how your business has conducted best practice regarding online security. This could be through providing staff training or having antivirus software, for example.

Just like any other insurance product, make sure you shop around and compare cyber insurance products to find a policy that suits your business.

Contact us to discuss your protection options.

IMPORTANT INFORMATION

Insurance coverage terms and costs will depend on individual circumstances.

This document is solely for information purposes and nothing in it is intended to constitute advice or a recommendation. You should not make any decisions based on its content.

While considerable care has been taken to ensure the information in this document is accurate and up-to-date, no warranty is given as to the accuracy or completeness of any information.