**Graphical user interface

Description automatically generated**

**Cyber-crime takes aim at the high-net-worth. Are your virtual assets protected?**

According to the National Crime Agency, cyber-crime costs the UK billions of pounds. As it continues to rise in scale and complexity, organisations and businesses have adopted more complex IT defences to counteract this. It means that **c**yber criminals are increasingly attacking high-net-worth individuals, viewing the wealthy as a far easier low-risk, high-return target.

**Vulnerability**

Visibility online, through business activities, charitable donations or social media postings, gives the hacker valuable profile information about you. Your phones, tablets and laptops – plus the welter of internet-connected devices now in the home offer a doorway into your daily and financial life.

Most cyber-attacks start with ‘phishing’. This is an email – or possibly a text or phone call – impersonating a friend, business associate or service provider. It is designed to trick you – or a family or staff member – into clicking a link that will download malware or ransomware or into sharing bank details or a password or, maybe, even into parting with money. Other cyber threats include ‘hacking’ often through your social media profile or email passwords, or through malicious software which can compromise your files, and hold these to ransom.

You may also be targeted indirectly by hackers through your businesses, family members, domestic and personal staff, financial and wealth advisers.

**Protection**

To protect yourself and your family it is sensible to follow certain simple basic principles:

* Ensure your operating system and security software always has the latest updates. This will help protect both the system and your financial data against malware.
* Regularly check that all your home network-connected devices, from refrigerators to smoke-alarms, have the latest protective firmware.  You are as vulnerable as your weakest network link.
* Use strong passwords – a combination of upper and lowercase letters and special characters are recommended. Also change passwords regularly, an encrypted password manager will help.
* Change the factory set passwords on both routers and any Mesh WI-FI equipment.
* Always back-up your data. It provides a solid defence against ransomware as the data is safe and accessible even if you lose control of a device.
* Manage your social media privacy settings. The less you share publicly the better.
* Make sure your children and any domestic or personal staff are aware of the need for internet security.
* Consider encrypting your data. An attacker is likely to give up on trying to decode gobbledygook.
* Install a virtual private network (VPN). A VPN will encrypt all traffic leaving your devices until it arrives at its destination. VPN is certainly a must if you log on to public Wi-Fi networks, particularly in airports or luxury hotels, which are happy hunting grounds for hackers of wealthy individuals.
* Finally, think carefully and check before responding to any email that looks slightly odd or has a link!

**Ricky Downs,** **Centor’s Private Clients’ Manager**

*“Recognising and understanding the various ways you may be a target of cyber-crime is an important first step in protecting your family and assets, however, some attacks do get through, which is when you will need exceptional personal cyber insurance to help mitigate any damage.”*

For more information contact Ricky on **020 7330 8725** or **rjd@centor.co.uk**