Online Security Guidance

MACINTYRE
WEALTH MANAGEMENT

We take our responsibility to look after your money, information and privacy seriously. We therefore have security measures in place to help combat fraud and cybercrime. As individuals there are also some simple steps and guidance that we can all easily follow to improve our personal online security:

SECURITY CHECKLIST:

Password protect devices and online accounts
Where possible, passwords should be at least eight characters long, include different types of characters, and should not be a proper word, name or place. Consider using phrases, a number of unconnected words or letters from something memorable to you but difficult to guess. Change your passwords regularly where possible, using different passwords for different accounts. Do not let anyone else know your password.

Beware of email and telephone scams
Unexpected emails may be malicious; containing viruses, malware or other tools criminals use to gain access to your information. Do not reply to an email or phone call asking for sensitive information, open an unexpected attachment or enter information into a website that you are directed to by a hyperlink. Instead, use a search engine to direct you to the organisation's login page.

Keep your operating system, firewall and antivirus up to date
Cybercrime is a fast moving industry. By keeping your systems up to date, they will be more resilient to new cyber-attacks. Also run regular virus scans of your computers and devices.

Be careful when using unsecure wireless connections
If you are unsure whether the connection is secure do not enter sensitive information into the device. If you are in a public place such as a café or hotel, the wireless connection is less likely to be secure.

Be aware of the risks associated with social media
Cyber criminals will use social media to look for your date of birth, place of birth or middle name, for example, which they can use to take over your accounts or commit identity theft. Use the privacy settings on websites and be careful about what you make publically available. Be aware of what your friends and family post about you.

OUR INTERACTIONS WITH YOU:

We will:
- Provide a secure website to login to Online Services (this can be checked by looking for the padlock icon next to the address bar).
- Only send withdrawal funds to a verified bank account in your name.
- Verify who you are when speaking to you on the phone, by asking you security questions.

We will not:
- Ask you for your password over the phone.
- Send you an unsolicited email with a hyperlink to our login page asking you to enter your Online Wealth Account credentials.
- Ask you for payment or credit card details.
- Call you to notify you of a problem, and then request you call us back immediately to discuss the problem further.

If you would like further information about online security and fraud, please visit www.getsafeonline.org, www.actionfraud.police.uk and www.cyberstreetwise.com*

**St. James's Place cannot accept responsibility for content on external websites.*