From: Kristina Temel
To: Kristina Temel
Cc: Alicia Wright
Subject: Cyber security
Date: Monday, 22 May 2017 5:28:41 pm
Attachments: image001.jpg

Dear Party Secretary,

Recent events overseas remind us that politicians, political parties, and public sector agencies can be targeted online and need to be mindful of cyber security. Below are some general points on security steps that we can all put in place to protect ourselves online and to avoid unauthorised access to personal information and our systems.

- **Digital footprint**
  Whenever you use the internet or other people publish information about you or your activities online, it leaves behind a footprint that may help others identify your interests, activities or locations you regularly attend. Use a search engine to review what information is already out there about you online and review the sensitivity of that data.

- **Think before you share**
  Both personal and company/organisation information can have intrinsic value to people looking for ways to exploit systems or get access to places they shouldn't be allowed. Consider carefully every request by email, text or phone for sensitive data that shouldn't be shared widely. Social media platforms can also be a treasure trove of information so make use of privacy settings to lock down access.

- **Use strong passwords**
  Passwords remain a sore point for end users struggling to remember a growing array of logins but are highly after sought by attackers. Complexity through mixing characters sets or overall passphrase length can help defend against determined attacks. Best practice is to never use the same password for more than one account or system and avoid sharing them. Investigate password manager software to help you create and store strong passwords that are too hard to remember.

- **Turn on two-factor authentication**
  Multi-factor authentication offers more security over a simple password and requires an attacker to know both your password and have access to your phone or a hardware token that must be used to login. Many companies now offer this form of increased security at no extra cost and layering your defences can be beneficial.

- **Travel securely**
  Your travel movements may also be of interest to other people keen to monitor your activities. Avoid posting information online that signals you will be away from your home or office for a long period of time, attackers may see an upcoming foreign trip as the perfect opportunity to access that location or send spoof emails to friends or colleagues that coincide with you being overseas. Avoid taking sensitive information on devices when you travel and be aware that leaving location services turned on may give away your location when using certain mobile apps.

- **Patch, patch and patch again**
  Keep your systems and software up to date to address emerging vulnerabilities; automate updates where feasible or apply patches as soon as you can. Surfing the internet with an old web browser can leave you open to attacks such as 'drive-by downloads' or 'malvertising' that let an attacker gain a foothold on your computer for further exploitation. Disable untrusted Microsoft Office macros as this software feature can be used to download malware.

- **Back up important data**
  Technology has improved over the years, but creating copies of your essential information can protect you against system failures or data being encrypted via ransomware and ensures you still have access to your files. Storing information both offline and in the cloud can provide a belt and braces approach to give you a range of options if the worst happens.

- **Hold onto your hardware**
  Losing a laptop or smartphone is one of the most common ways for data or credentials to be compromised and it can cost significant sums to replace items too. Password protecting devices and using encryption methods to scramble the data stored within them can prevent your information from being accessed if they fall into the wrong hands. Smartphones often come with ways to track and/or remotely wipe them if they are lost or stolen and there are similar tools you can use to protect larger computers.

- **Restrict admin privileges**
  An administrative user on a system can add or remove software and may also give permissions to programmes to perform unwanted actions that could, for example, allow an attacker to remotely access your data or view your webcam. Use an admin level account to maintain the computer but create a basic level login to use when simply checking email or browsing the web.

- **Be careful using free Wi-Fi**
  A mobile worker needs to access information anywhere and everywhere and free Wi-Fi can be a tempting way to trim data costs when travelling. Unsecure networks may reduce the security of your communications though and it's important not to access sensitive systems or send private messages over insecure connections. Consider a VPN solution to add a protective layer that prevents your data from being intercepted.

There are several organisations who can provide advice and assistance to help keep you and your information secure online. They include the recently established CERT NZ, the National Cyber Security Centre and Netsafe.

CERT NZ can be contacted by phone on 0800 CERT NZ (0800 2378 69) - https://www.cert.govt.nz. They provide a central point of contact for reporting cyber incidents and advice on how to protect yourself and your systems from most cyber threats.

The National Cyber Security Centre (NCSC) can be contacted by email to info@ncsc.govt.nz or by phone on 04 498 7654 - https://www.ncsc.govt.nz. The NCSC is part of the Government Communications Security Bureau. Its focus is on helping to protect New Zealand's most significant organisations and systems, through the provision of information security guidance, standards, and support in the management of significant cyber security incidents.

Netsafe can be contacted by email to queries@netsafe.org.nz or by phone on 0508 NETSAFE (0508 638 723) - https://www.netsafe.org.nz. Netsafe provides a range of information and advice on protecting yourself from more common forms of cyber threat.

Hope you find this of assistance.

Kind regards

Kristina Temel

Enrol to Vote

Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri
PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | http://www.elections.org.nz