Answers to your questions

Passwords

- **Are password managers safe to use?**
  - Yes. Password managers are a safe way to create and maintain long, strong, and unique passwords. You can make your password manager even safer by enabling two-factor authentication on it. Password managers should be storing your passwords in an encrypted format so even in the event of a data breach, your data should still be safe.

- **What are your views on saving passwords in web browsers?**
  - Saving passwords to your browser essentially turns your web browser into a password manager. This means that you need to treat your browser with extra caution, because anyone who uses it will have access to all your passwords. Make sure your browser has a long, strong and unique password and turn off 'auto-login' options. If your device has two-factor authentication to use saved passwords – including fingerprint, face ID – turn this on as well.

Phishing

- **Should you report these phishing emails/texts to the company that it allegedly comes from? Does it help them?**
  - This can help them to be aware that their brand is being used in a phishing campaign. At CERT NZ we have worked with several organisations who have their brands used in phishing campaigns. If we see an increase in the volume of phishing misusing their brand, we get in contact with them so they can warn their customers and other stakeholders. We can also take actions against the malicious links contained in phishing. You can report phishing to CERT NZ through our site at phishpond@ops.cert.govt.nz.

- **Should you delete phishing emails?**
  - Yes! Once you have reported that phishing email to CERT NZ at phishpond@ops.cert.govt.nz, you can safely delete phishing emails from your inbox. Some email systems also allow you to mark a message as phishing, which may help identify them automatically in the future.

- **Is it possible to find the IP address of someone emailing phishing emails?**
  - Yes, it is possible to capture an IP address from an email, however this isn't always accurate. For example, scammers will commonly use VPN software to mask a user IP address.

- **If you see a link to unsubscribe on an email, is it safe to do so?**
  - Unsubscribe links are common with marketing emails and spam. It's important to check that link out first, hover over the 'unsubscribe' button with your mouse (press and hold if you are on a mobile phone or tablet) so you can see the full link. If the

link looks genuine to that organisation, you can click on the 'unsubscribe' link to stop further marketing emails being sent to your inbox.

- **If I have clicked on the links from text messages by mistake, would it hack my phone by just clicking on them?**
  - In most cases, you aren't at risk by simply clicking on the link contained in a phishing email or text. However, in a small number of cases, we do see attempts to install malware through these malicious links. Keeping your operating system up to date is a great way to help prevent these kinds of 'drive-by' downloads. Additionally, if you have an Android device, ensure the "unknown sources" system setting is switched on. Doing so will mean you can only install things to your Android device, via the Play Store.

- **Quite often generic emails of companies use different domain names in the email than that of the website. Is there an easy way to check if the email domain is legit?**
  - Companies can often use a range of different email address, but typically those email addresses will have the same 'domain' after the @ symbol. For example info@cert.govt.nz, comms@cert.govt.nz etc. Sometimes organisations will list on their websites the genuine email addresses/domains they use, to help you determine if an email is genuinely from them. If you are concerned about an email and haven't been able to determine if it is genuine, you can always contact the organisation directly to confirm an email's authenticity.

Updates

- **How can you tell that updates are legitimate?**
  - The best way to ensure updates are genuine is to get those direct from the company that makes the software and through appropriate channels. For example, updates to your Windows operating system should be installed through the settings of your device. Updates to Google chrome should be initiated through the settings of the Chrome browser. Updates to apps should come from the Play Store or App Store etc.

Backups

- **What about hybrid option to use cloud backups and actual encrypted external hard drive? Is this wise?**
  - Backups are a powerful security measure to help your recovery in the event of a cyber security incident. How you do backups for your business will depend on the size and scope of your business. You might consider a cloud backup service, to make things a bit easier for you or doing backups yourself through something like a physical hard drive. If having both options in place is beneficial to your organisation and you have the capacity to do so, there is no harm running both backup processes in conjunction with one another. This will also give you an alternative backup option; if your physical backup is damaged you can restore from your cloud backup, and vice versa.

Reporting

- **Can you report a scam which was a couple of years ago?**
  - Yes. You can report a scam that happened at any point in time. This can help us to stay aware of the risk and threats that are affecting New Zealanders. If there are any websites that are a part of that scam, and they are still live, we may still be able to act against that site too. You can do that here: https://www.cert.govt.nz/individuals/report-an-issue/

Contacting us

- **Is there an area with CERT NZ that we can subscribe to, to see what the upcoming webinars are?**
  - Yes! Please subscribe to our business updates here: https://www.ownyouronline.govt.nz/subscribe/subscribe-business/ By signing up to this list, you'd get the latest online security news and alerts straight to your inbox – this includes upcoming webinars!