29 MARCH 2021

Scammers hop into Easter with hollow promises set to cause pain

Netsafe numbers shows a 360% jump in online incidents during Easter break since 2017

It is around this time of year the community is justifiably urged to be cautious on the road. And this year, Netsafe is also warning people to be careful when it comes to online scams.

Easter is when the internet is most dangerous – compared with the rest of the year – in terms of scammer activity.

Insights from New Zealand's leading online safety experts found it is not just the Easter Bunny working during the April break.

"During Easter, many people connect online with whānau and hoa and share special memories on social media," says Martin Cocker, Netsafe CEO.

"However, when Netsafe examined data spanning the previous four Easter periods, we identified reports of online incidents had gone up 360 percent, and they mostly related to scams."

Some of the common scams Netsafe has found to be prevalent during Easter include:

- Online shopping
- Prize or promotional scam
- Phishing[1]
- Debt collection for non-existent bills

"It can be hard to get your head around this data because the idea that anyone would intentionally cause harm during a holiday such as Easter doesn't sit well with most people," Cocker says.

Netsafe was also highly concerned to see a considerable proportion of reports it handled last Easter (52.9 percent) related to "fake sextortion"[2].

Cocker says this statistic may be high because of the Alert Level 4 Lockdown during Easter 2020. International scammers became cognisant more people were at home online and set about targeting New Zealand.

"Scammers are criminals who work around the clock to invent webpages, adverts and emails

---

[1] A fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card numbers.

[2] A scammer falsely claims to have hacked into a person's device and recorded intimate recordings of people using porn websites. The email threatens to release the video to their contacts unless the victim pays them a sum of money. In some versions of this scam, the scam email subject line also includes the victim's password that they use (or have used in the past) for their online accounts.

with the same objective in mind, and that is to rip people off and potentially steal their private details."

Netsafe has developed advice specific to the Easter holiday and produced tips for people who want to stay safe online at netsafe.org.nz/holidayscams.

"So, it's a good reminder to be extra vigilant to unsolicited emails or giving personal information such as financial details."

Netsafe's 10 tips to scam spotting

An online scam is any scheme designed to trick people out of money or steal their personal information that uses, or is delivered via, digital communications. Here are a few tell-tale signs you might be being scammed:

1. **Contact that is out of the blue** – even if the person says they're from a legitimate organisation like the bank, an embassy or your internet provider
2. **Getting told there's a problem with your phone, laptop or internet connections** – often they will offer to fix your device or say they are from your phone or internet company
3. **Being asked for passwords** – legitimate organisations will never ask for the passwords to your online accounts
4. **Needing to verify your account or details** – don't respond or click on any links in the communication even if it looks like it's from a real organisation
5. **Trying to get you to move outside of an online trading or booking website or app** (like Air BnB) – don't pay outside of the normal website or app processes
6. **Offering money or a prize in exchange for something up front** – they might say that it's a processing fee or something similar
7. **Being asked for money by friends/partners you've met online** – this is a common tactic, and you should never pay the money without getting advice from someone first
8. **Unusual ways to pay for something** – scammers try to use payments that can't be traced such as pre-loaded debit cards, gift cards, bitcoins, iTunes cards or money transfer systems
9. **Asking for remote access to your device** – never do this unless you have actively sought out the service they are providing
10. **Pressuring you to decide quickly** – this could be to avoid something bad (e.g. an account being closed) or to take advantage of something good (a deal or investment)

-Ends-

Media contact

Angela Boundy – Senior Marketing and Communications Advisor

+64 27 228 3930 | angelab@netsafe.org.nz

About Netsafe

Netsafe is an independent non-profit organisation with an unrelenting focus on online safety. We keep people of all ages safe online by providing free support, advice and education. Visit netsafe.org.nz for valuable resources or call 0508 NETSAFE (0508 638 723) seven days a week for help with an online incident. Netsafe is open during Easter between 9 am and 5 pm.