GeekSafe™ Newsletter

Issue 20

Hi Me!

Welcome to the 20th issue of the GeekSafe™ newsletter, packed with important information to help keep you and your devices safe online!

With Netsafety Week taking place, this edition of the GeekSafe newsletter will focus on helping you stay secure in an increasingly digital world. We're

addressing common misconceptions about iPhone security, highlighting a circulating Spotify phishing scam, and providing some tell-tale signs for spotting AI-generated phone call scams. We'll also share Netsafe's new SCAMS checklist tool, which we think is an excellent resource to have in your toolkit when evaluating the legitimacy of suspicious emails, texts, calls, and more!

Don't forget, if you ever receive any suspicious emails or other electronic messages, you can forward them to [redacted] Simply follow the instructions at the bottom of this email.

Can't figure out how to forward a suspicious message or did you get a scam call you want to discuss? - Send an email to [redacted] letting us know, and one of our GeekSafe™ team will give you a call back to discuss.

The GeekSafe™ Team.

Netsafety Week - SCAMS checklist

Image source: Netsafe

We recommend that you ask yourself these questions when evaluating whether suspicious content is legitimate or not!

As our day-to-day lives become digital, scams unsurprisingly continue to grow. But with more scams, come more handy tools and up-to-date information that help us to recognise and respond to suspicious activity safely.

One great example is Netsafe's new SCAMS checklist which they shared during their Netsafety Week campaign. A very handy reminder of the key context clues that can help you spot something that's not quite right.

S – Surprise? Is the message out of the blue? Are the contents of it about something you aren't expecting (such as a renewal, account deactivation etc.)?

C – Control? Are you being rushed to act? Scammers will often push for urgency. This is an attempt to make you act quickly so you don't take a second to pause and think about the

legitimacy of the message.

A – Access? Is the person asking for passwords, personal details or remote access? This is a common scam tactic. Legitimate organisations like your bank will never ask for PINs, passwords, or full card details over the phone. They'll use other ways to verify your identity, such as basic security questions or two-factor authentication.

M – Money? Requests of any kind of payment, whether that be basic debiting, gift cards or crypto is a strong signal of a scam.

S – Stop and get support. If you suspect you're dealing with a scam, or aren't quite sure, don't engage further. Seek advice using your GeekSafe membership!

Recognising AI-generated phone call scams!

A common tactic scammers use to deceive victims is voice cloning. This technique involves using AI to generate a voice that closely mimics a specific person.

Scammers are aware that when it comes to family or friends, or anyone else we know and trust, that we won't bat an eye when they "call for help" or "ask a favour".

Because of AI's ability to clone voices, it's our recommendation that you first and foremost organise a safe word with close family and friends. That way, if you get a strange call from a loved one asking for money, you can immediately confirm the calls legitimacy!

Otherwise, check out these great tips for pin-pointing an AI-generated phone call scam.

- **The background noise sounds off.** For example, is there oddly no background noise at all? Or, does the background noise sound unnatural, with static or crackling noises?

- **The speakers voice sounds robotic.** Are there unnatural pauses in the call? Or, is the speech too broad and/or repetitive? If the speaker's voice sounds mechanical, flat or simply too perfect, you're likely talking to AI.

- **Inconsistencies in the caller's story.** Pay close attention to what the caller is saying. For example, did your "daughter" claim she *lost her phone* only to then say *her*

phone was broken later in the call?

- **Other tell-tale signs of a scam.** Always consider your usual tell-tale signs of a scam. Is the caller putting pressure on you with a time frame? Are they making unexpected requests for personal or financial details? Is the call coming from an unknown or overseas number?

Who has fallen victim to a scam more? iPhone or Android users?

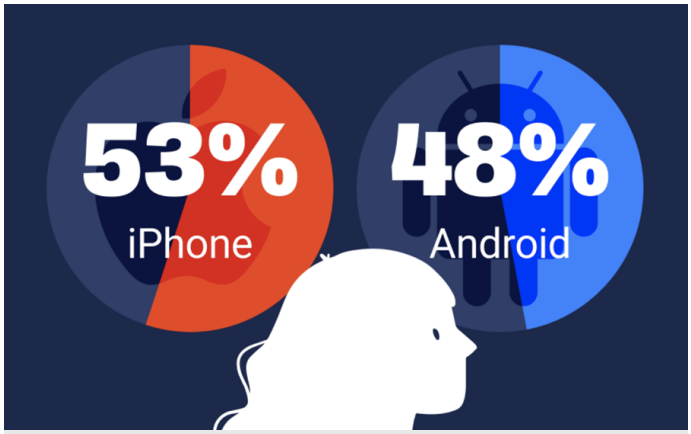


Image source: Malwarebytes

New analysis from Malwarebytes reveals that iPhone users may be falling behind Android users in terms of cybersecurity.

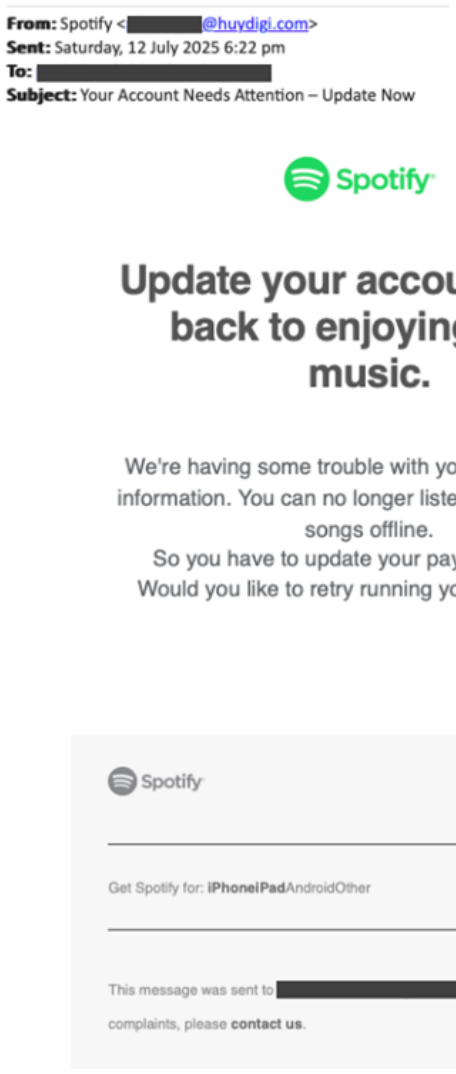
There's a common misconception that Apple users are immune to online threats. Especially when compared to their competition, such as Windows and Android. But this latest study proves that owning an iPhone doesn't

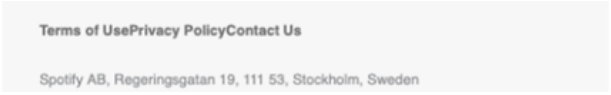
guarantee complete safety.

This recent analysis found that Apple users are guilty of engaging in more risky online behaviour, take fewer precautions online and are more likely to be the victims of scams.

What this tells us is, no matter your device, everyone should **create unique, long and strong passwords** for each of their online accounts and **seek friends and families advice** when something doesn't feel quite right.

Recent Scams





Spotify phishing email - Your account needs attention!

We've been sent this "failed payment" Spotify phishing email a few times now, so it's clear to us it's making rounds in people's inboxes.

While the exact goal of this scam isn't clear, since there's no obvious link or button for the recipient to click, there are still a few red flags that reveal it's a scam.

- The sender's address does not end in @spotify.com

- The layout of the information at the bottom of this email is jumbled and lacks proper spacing between words.

Ransomeware attacks on Kiwi businesses

Ransomware attacks are when malicious actors gain access to your device and data through malware and lock your files and computer.

The attackers will then ask for a ransom to unlock these files.

Whilst most of these recent attacks have been targeting businesses, it is a great reminder that everyone should be backing up their data.

Ensure you have **regular backups** of your data that are stored securely and **not left plugged into your device**.

How to forward suspicious messages?