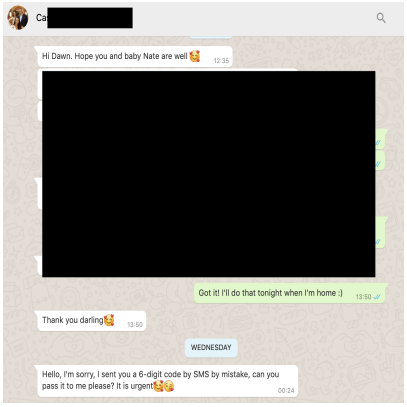


How To Protect Yourself From Scams While Shopping Online

Description

With more people staying home and carrying out more online transactions this year, there are also more bad guys using the Internet to scam people. In fact, more than $157 million has been lost to scammers in the first 8 months of 2020, with the most common being e-commerce scams, social media impersonation scams and loan scams.

I nearly fell prey to one such scam myself last week when a friend sent me this:

[redacted]

pe you and baby Nate are well 🥰 12:35

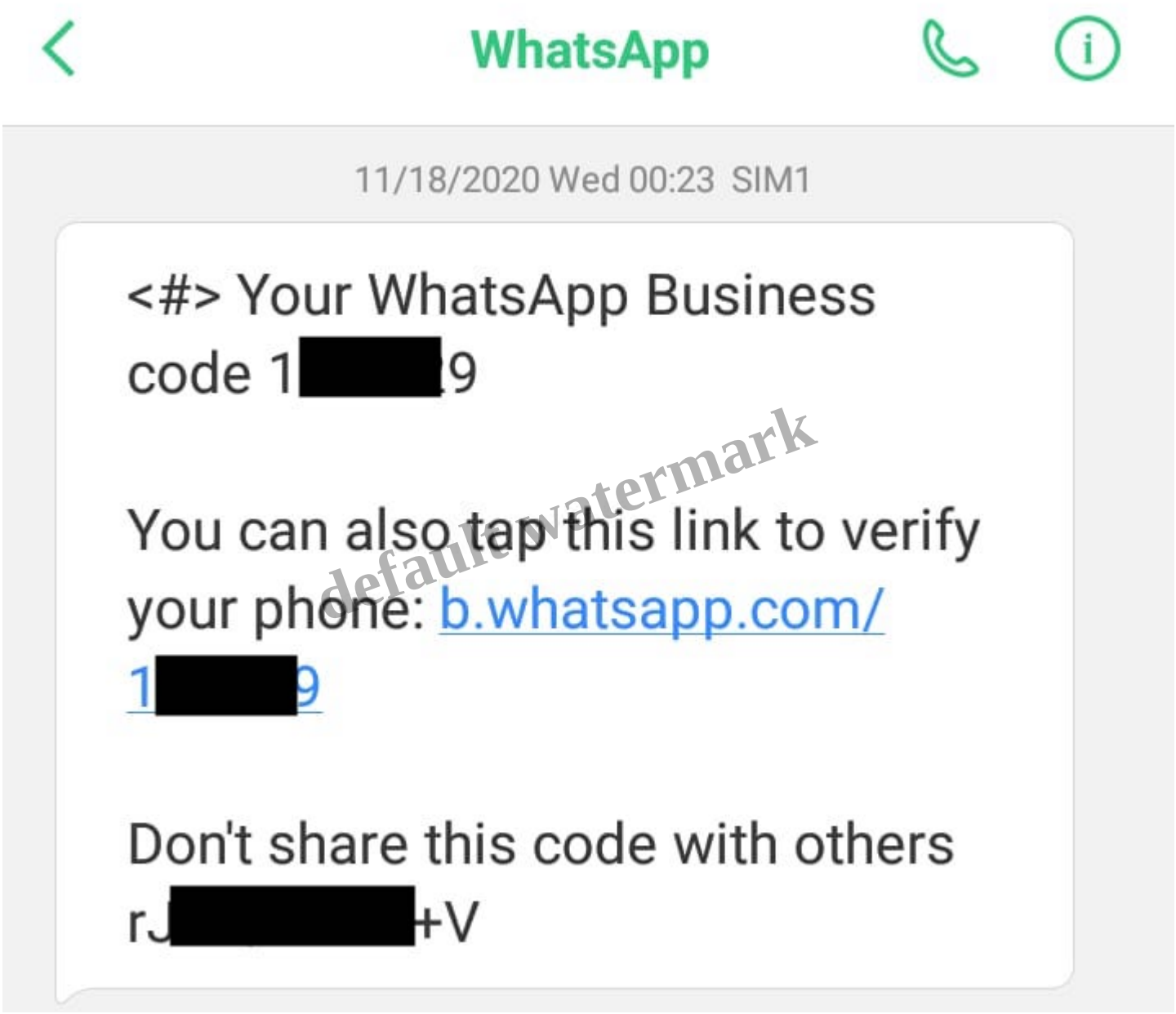
[redacted]

Got it! I'll do that tonight when I'm

arling🥰 13:50

WEDNESDAY

The scammers managed to replicate her tone of voice, her style of writing and emojis…so well that I had no reason to suspect her account had been hacked. Given this and her urgency, it sounded legitimate.



This was the SMS I received.

I've helped a friend change his account to a WhatsApp Business version before, and recalled the process involved such a verification code. The funny thing is, her number looks VERY different from mine, so it seems a little odd as to how she would have inputted mine by mistake instead.

I wasn't sure if this was a scam, but eventually reasoned that if my friend had really sent the code to me by mistake, she could easily just reset again on her end, even if I don't give it to her.

A day later, I saw this AsiaOne article describing the exact same technique and confirming my suspicions.

That was when I realised, anyone can easily become a victim of online scams. It doesn't matter whether you're educated or digitally savvy, because the scammers are getting smarter and evolving their techniques as they go along.

There have also been contact tracing scams during this COVID-19 period.

Hence I'm writing this piece to raise more awareness. If you've not experienced anything like that yet, here's how the most common scams look like, and what you can do to protect yourself from becoming the next victim.

E-commerce Scams

Could you spot a Carousell scam if you came across one? It isn't that easy – click to see some examples in this article. Or how about a Grab scam?

Not only are scammers putting up scam listing on popular online shopping portals, they are also masquerading as "legitimate" merchant websites. They do this by creating phishing websites and other malicious web pages that are designed to look like the websites of actual retailers that you visit.

Some will even run Google SEO ads to make you click into their websites instead of the actual retailer you're trying to visit!

They'll also post fake deals on social media such as Facebook and Instagram (read how 300,000 people fell for this ASOS scam), or send you emails disguised as the retailer (click to see an example).

Emails are probably one of the main ways your favourite stores and retailers will communicate with you during busy shopping seasons like 11.11 or Black Friday, and unfortunately, scammers are aware of this too. Be smarter than them. And if a deal is too good to be true, there's a high chance it could be a scam.

Social Media Impersonation Scams

According to the Singapore Police, they received at least 1,000 reports of such scams amounting to at least $2.2 million, in the first 5 months of 2020 alone.

In the majority of these cases, victims were tricked into disclosing their credit card information and One-Time Password (OTP) to scammers. This scam works because scammers prey on your TRUST when you receive a request from your friends or family members. So please verify with them directly *via another mode of contact* before you give away anything.It can take many forms, such as asking for your personal information on the pretext of signing up for fake contests or promotions on Lazada or Shopee.

Loan Scams

If you've received any SMS or message advertising loan services, betting services or investments…stay far, far away.If you really need a loan, get them from authorised financial institutions and not from such scammers / strangers.

Here's what Philip Doyle, Head of Financial Crime at Revolut had to say:

> It is very exciting when we stumble upon a deal with an unbelievable discount and, on days like Black Friday or Cyber Monday, it's easy to get swept up in all the hype. That's exactly what scammers are relying on.Besides making your purchases through trusted merchants, remember to take steps to protect your details and be aware of any phishing scams out there.
>
> If you want to be extra safe, Revolut's disposable virtual card gives you the convenience of a debit card, but it generates new disposable card details for each purchase, providing you with an extra-secure solution for making online payments at merchants you do not know or trust.

Tips on how to avoid becoming the next scam victim:

- Never give out your banking information or OTP to anyone, ever!
- Incoming calls with +65 are NOT from Singapore, but are in fact overseas calls disguised as a local Singapore number. Don't bother picking it up as it is likely to be an overseas scammer.
- If you get any calls or email from an "official" body that does not address you by your name, it is likely to be a scam.
- Watch out for callers who ask you to download a certain software or app so that they can "help" you fix the fake problem. You could be handing them the remote control keys to your device instead.
- Always head DIRECTLY to the retailer's website instead of searching for it through Google / search engines. This will help you avoid the fake search engine ads that scammers put out.
- If you're buying from an online portal, check if the seller has been verified, or at least read the seller's reviews first.
- Be wary when clicking links in emails, and always hover over the link first to check if it is legitimate.
- Do not click on URL links provided in unsolicited text messages.
- If you've stopped receiving calls or texts recently and you don't know why, check with your telco to make sure you haven't been a victim of a SIM swap.
- If you see any suspicious transactions on your credit card statement that you don't recall making, clarify with your credit card company right away. *(Even if it turns out you simply forgot about a certain transaction, it is better to be safe than sorry.)*

- Consider using disposable virtual cards (such as Revolut) for online payments and which self-destructs after being used once, and generates a new set of credit card details for your next transaction.

If you're using an iPhone, you can also download the **ScamShield app** here, which is by the National Crime Prevention Council and works in the background to filter/block scam messages and calls from numbers used in illegal activities. Unfortunately, there isn't an Android version yet.Share this article with your friends and family so they can be better educated on common scam tactics and not fall for them.

But remember, scammers are also evolving as we speak. They are becoming smarter at disguising themselves and looking increasingly legitimate. By the time a scam tactic has been confirmed and announced by the police, it might be too late as there would already have been victims.

I'll continue to post on scams on this blog (read about previous scams here, here, here and here.)

So protect yourself by always being vigilant while shopping online.

With love,
Budget Babe
Category

1. Savings