@CCoFiji Consumer Council of Fiji www.consumersfiji.org Mobile App

20 January 2023 FEATURE

Sharing is Caring, unless it is your One Time Password!

The evolution of the internet has created fantastic means to explore new topics, staying connected with loved ones and purchasing favourite products and services with just a few clicks and swipes. But it does come with a few potential dangers; namely, online scams. This type of scam has increased significantly in the past. With that in mind, the Council is once again, reiterating on the need for consumers to remain vigilant when surfing through the internet and protect their mobile wallet information and account details at all costs.

In today's time and age, it can become extremely difficult to determine which businesses operating online are genuine. The global proliferation of the internet has allowed con artists to expand their craft to different markets and reach previously untapped consumers. Many times, the con artists' creative marketing often results in consumers being duped out of their hard-earned cash with little to no possibility of redress. As we progress further into the new year, it is no secret that online shopping has become an integral part of daily life. With busy schedules, heavy traffic, and the effort required to run errands in person, online shopping offers convenient options. However, it is important to be aware of potential risks, such as losing money if you are not careful when making online purchases. As the volume of online orders continues to grow, scammers have found new ways to exploit people.

What are online scams?

Online scams, also known as internet scams, continue to evolve and can vary widely. The term generally refers to someone using internet services or software to defraud or take advantage of victims, typically for financial gain. Cybercriminals may contact potential victims through personal or work email accounts, social networking sites, dating apps, or other methods in attempts to obtain financial or other valuable personal information.

Many successful scams on the internet have similar endings; the victim loses their own money or fails to receive funds the cybercriminal promised. In worst-case scenarios, the victim might even lose their identity. While this has not been the case in Fiji, there is no evidence to suggest that we are not heading in that direction considering the high number of online scams occurring on a daily basis.

What is a One Time Password (OTP) scam?

A common practice that is slowly crept into the highly digitalized world is One Time Password Scams, or simply known as OTP scams. Many websites now require that you provide a password and a numeric code called an OTP or "one time passcode" that is sent to you via a text message or email. This increases security since if your password gets stolen, fraudsters still cannot access your account on the site without the time-sensitive passcode.
But fraudsters are now getting around that requirement by calling and pretending to be a legitimate organization such as the post office, bank or other trusted organization and asking

for the OTP that was just delivered to your phone by text or email. Sometimes fraudsters will even pose as bank investigators who are calling about a suspected fraudulent transaction. Unfortunately, many consumers fall for this gimmick and end up sharing the OTP.

Simple tips to avoid the scam:

• Never share an OTP with anyone who calls you, texts you or emails you asking for the code. The OTP sent to you is personal and unique to you. We have always been told that sharing is caring. But there are some things that you can never share with anyone and your OTP should always be at the top of the list.

• Remember that your bank or any other reputable company will never ask you to share an OTP with them over the phone, by text or by email.

Case Study:

The Consumer Council of Fiji has received reports of unauthorized withdrawals from people's mobile wallet last year where scammers were able to convince consumers to share their 'One Time Password' through certain gimmicks such as winning a lottery. In one of the cases, a consumer (complainant) received a call from an alleged scammer claiming she has won a lottery and was required to provide her e-wallet details for the transfer of the winning cash prize. While being on call with the scammer, the complainant was told that she would soon receive a text message (containing one-time-password) on her mobile; and she would be required to provide to the caller the same text message (one-time-password) for the transfer of the winning to which the complainant complied. Nevertheless, soon after this, $100 was transferred from her account and withdrawn.

What to do if you have been caught in a data breach?

Banks and other financial institutions take extensive steps to protect your personal information entrusted to them and to help you protect it as well. If you think you have been the victim of an OTP scam and have provided your financial information to a fraudster, contact your financial institution immediately.

Do's and Don'ts for passwords and PINs

- Never use the same (or similar) password or PIN for more than one service.
- Do not use a single dictionary word (e.g., "Cardboard1") as a password. Two unrelated words ("CardboardDog1") is easier to remember and much harder to crack.
- Keep it impersonal. Avoid easy-to-guess details such as family or pet names.
- Make it unusual. A quick web search will tell you if your new password or elements of it are featured on any 'most commonly used passwords' lists that do the rounds a few times a year.
- If you write your login details down somewhere, make sure it is a safe place and out of sight.

If you come across similar scams, please report the matter to the Council on toll-free number 155 or lodge a complaint using the Consumer Council of Fiji mobile app or the Consumer Council of Fiji website.