SECURITAS INTELLIGENCE UNIT

Take Five – COVID-19 Scams

11 August 2020

Overview

Fraudsters continue to use the COVID-19 pandemic as an opportunity to exploit people. They use sophisticated methods to manipulate innocent victims, impersonating government sites, NHS Test and Trace operatives and well-known subscription services to get people to part with their money and personal information.

The banking and finance sector is working with the government and law enforcement to help identify scams and prevent people becoming victims of fraud.

The 10 most reported scams to Action Fraud

Covid-19 financial support scams

- **Fake government emails** designed to look like they are from government departments offering grants of up to £7,500. These emails contain links which steal personal and financial information from victims
- Emails offering access to **'COVID-19 relief funds'** encouraging victims to fill in a form with their personal information to score for or gain 'fast access' to money.
- **Council tax reduction emails.** These official looking emails, which use government branding, contain links which lead to a fake government website which is used to access personal and financial information.
- Benefit recipients are being targeted with offers to help them apply for **Universal Credit**, while taking some of the payment as an advance for their "services".

Health scams

- Imitating the **NHS Test and Trace** service, criminals are sending phishing emails and links claiming that the recipient has been in contact with someone diagnosed with COVID-19. These links direct the recipient to fake websites that are used to steal personal and financial information or infect devices with malware.
- Online **fake adverts** for COVID-19-related products such as **hand sanitizer and face masks** which do not exist.

Lockdown scams

- Fake emails and text messages claiming to be from **TV Licensing**, informing people they are eligible for six months of free TV licensing because of the coronavirus pandemic. Victims are being told there has been a problem with their direct debit and are asked to click on a link that takes them to a fake website used to steal personal and financial information.
- **Online TV subscription services** have seen a rise in viewers during the lockdown, customers have been targeted using authentic looking emails asking them to update their payment details by clicking on a link which is then used to steal credit card information.
- Users of **online dating websites** are being targeted by criminals who create fake profiles (sometimes using the identities of real people) on social media sites to manipulate victims into handing over their money.
- Social media websites are being used to advertise **fake investment opportunities**, encouraging victims to "take advantage of the financial downturn". Bitcoin in particular is used to encourage unsuspecting victims to put money into fake investment companies using fake websites.

Take Five – COVID-19 Scams

Take five to stop fraud

People are being encouraged to "take five" before opening or entering information in any link sent via email. Remain vigilant, **Stop**, **Challenge** and **Protect** when receiving any messages out of the blue.

- **Stop:** Take a moment to stop and think before parting with your money or information, it could keep you safe.
- **Challenge:** Could it be fake? Remember it is ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** Contact your bank immediately if you think you have been a victim of a scam and report it to Action Fraud.

Other tips for identifying possible scams

- The website address is inconsistent with that of the legitimate organisation.
- The email address matches the name of the sender.
- The phone call, text or emails asks for financial information such as PIN, passwords.
- You receive a call or email out of the blue with an urgent request for your personal or financial information, or to make an immediate payment.
- You are offered a heavily discounted or considerably cheaper product compared to the original price.
- There are spelling and grammar mistakes, or inconsistencies in the story you are given.

If you have any questions regarding the content of this report, please contact the ***Securitas Intelligence Unit***.