Avoid scams during the Coronavirus outbreak

Hampden & Co. BANKERS

Fraudsters prey on people's anxieties and fears about COVID-19. Please be on high alert for scams and always stop to think before parting with your money or your information.

The top 10 COVID-19 scams (published by UK Finance July 2020)

Financial support scams	1. Criminals have sent fake government emails designed to look like they are from government departments offering monetary grants. The emails contain links which steal personal and financial information from victims.
	2. Fraudsters have been sending scam emails which offer access to 'COVID-19 relief funds' encouraging victims to fill in a form with their personal information.
	3. Criminals have been targeting people with official-looking emails offering a 'council tax reduction'. These emails, which use government branding, contain links which lead to a fake government website which is used to access personal and financial information.
	4. Fraudsters are preying on benefit recipients, offering to help apply for Universal Credit, while taking some of the payment as an advance for their 'services'.
Health scams	5. Criminals are sending phishing emails and links claiming that the recipient has been in contact with someone diagnosed with COVID-19. These lead to fake websites that are used to steal personal and financial information or infect devices with malware.
	6. Victims are being targeted by fake adverts for COVID-related products such as hand sanitizer and face masks which do not exist.
Lockdown scams	7. Criminals are sending fake emails and texts claiming to be from TV Licensing, telling people they are eligible for six months of free TV license because of the coronavirus pandemic. Victims are 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.
	8. Amid a rise in the use of online TV subscription services during the lockdown, customers of these services have been targeted by criminals sending convincing emails asking them to update their payment details by clicking on a link which is then used to steal credit card information.
	9. Fraudsters are exploiting those using online dating websites by creating fake profiles on social media sites used to manipulate victims into handing over their money. Often criminals will use the identities of real people to strike up relationships with their targets.
	10. Criminals are using social media websites to advertise fake investment opportunities, encouraging victims to "take advantage of the financial downturn". Bitcoin platforms are using emails and adverts on social media platforms to encourage unsuspecting victims to put money into fake investment companies using fake websites.

How to prevent falling victim to a scam

STOP	Taking a moment to stop and think before parting with your money or information could keep you safe. Remember, Hampden & Co will never ask you to move money to a "safe account", or ask you for your PIN, the 3 digit number on the back of your card or a One Time Password
CHALLENGE	Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
PROTECT	If you think you've fallen for a scam, contact your banker immediately and report it to Action Fraud.

London Third Floor, 36 Dover Street, London, W1S 4NH. Tel: 020 3841 9922
Edinburgh 9 Charlotte Square, Edinburgh, EH2 4DR. Tel: 0131 226 7300