YH ROCU

**Yorkshire & Humber**
**REGIONAL ORGANISED CRIME UNIT**




# FAKE ONLINE CORONA VIRUS MAP DELIVERS WELL-KNOWN MALWARE

A malicious site pertaining to be a live map of COVID-19 cases is circulating the internet. The site infects the victim with the AZORult Trojan, this malware can steal sensitive data from the victim.

The site is being spread via email attachments, online adverts and social engineering. A search online for Corona Virus map may also navigate to this malicious site too.

> “Fraudsters are targeting users working from home to invest in bitcoin. Fraudsters try to deceive their intended victims by stating they can earn millions, which leads the victims to click on the fraudulent links.”

# COVID-19 ACTION FRAUD REPORTS

Recorded between 29-31st March.
These reports accounted for £240,226.43 of total losses. The highest loss was for £105,000.00. It was a mandate fraud in which the suspects used the corona virus as the reason for requesting the payment be made to an alternate bank account.

| Fraud Type | Number of Reports | Losses |
|---|---|---|
| None of the Above | 23 | £122,415.33 |
| Online Shopping and Auctions | 21 | £8,367.42 |
| Consumer Non Investment Fraud | 8 | £1,434.11 |
| Advance Fee Frauds | 6 | £0.00 |
| Computer Virus\Malware\ Spyware | 3 | £0.00 |
| Mandate Fraud | 2 | £1,700.00 |
| Ticket Fraud | 2 | £418.22 |
| Pension Liberation Fraud | 2 | £0.01 |
| Application Fraud | 1 | £105,000.00 |
| Other Financial Investment | 1 | £484.34 |
| Lender Loan Fraud | 1 | £224.00 |
| Door to Door Sales | 1 | £180.00 |
| Charity Fraud | 1 | £3.00 |
| Hacking - Social Media and Email | 1 | £0.00 |
| Grand Total | 73 | £240,226.43 |

# LATEST NCSC GUIDANCE

The NCSC has outlined recommended steps for organisations in:

- Preparing for home working
- Setting up new accounts and accesses
- Controlling access to corporate systems
- Helping staff to look after devices
- Reducing the risk from removable media

Within the guidance there is advice on dealing with suspicious emails, as evidence emerges that criminals are exploiting the Corona Virus online.
The guidance offers advice on spotting phishing emails and scams, as well as on how to respond in the event of falling victim to a scam.

## YHROCU ADVICE

Our key mitigation advice remains the same as always:

- Ensure your devices are running the most recent software (both your operating system and applications)
- Make sure your passwords are unique, use the NCSC guidelines on 3 random words to keep your accounts safe
- Consider activating 2 factor and multifator authentication to add an extra layer of security to your devices and accounts.
- Be wary of emails and text messages containing links and attachments. Try and avoid clicking on links in digital correspondence unless you can confirm the validity of the sender.
- Avoid using free WiFi hotspots without using a VPN to ensure your devices traffic is encrypted and harder for a criminal to intercept and read.