

Cyber crime - collateral damage from COVID19

Scammers are playing off our coronavirus fears for criminal gain. National Cyber Security Centre has removed more than 2000 online scams related to coronavirus, including:

471 fake online shops selling fraudulent coronavirus related items, 555 malware distributed sites set up to cause significant damage to any visitors, 200 phishing sites seeking personal information such as passwords or credit card details, 832 advance-fee frauds where a large sum of money is promised in return for a set-up payment.

Right now many are vulnerable to these scams, make sure you do not fall victim by taking the following precautions.

- **Make sure your virus software and your operating software is up to date.**
- **DO NOT click on any link from an unknown source, delete without opening**
- **Never open a e-mail from someone you do not know and trust.**
- **If someone is offering you money ask yourself why, how do I know this person?**
- **If the goods are too cheap and a real bargain ask yourself why?**
- **Generally speaking if its too good to be true then its FAKE**



EA3350