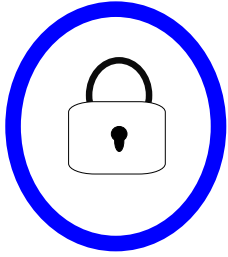




Mental Health Information Station Tips for Protecting yourself against cyber crime

COVID-19 has meant that we are all spending more time at home and online. Unfortunately criminals will use every opportunity they can to scam innocent people and businesses

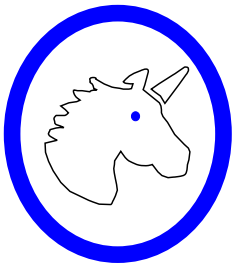
Here is a handy checklist to ensure that you don't become a victim



Before it happens - Keep Your Information Close - Social Media and publicly available information allow criminals to make scams increasingly personalised. By practising safe online sharing practices you can have a firstline of defense against scammers. Remember it is OK to challenge an unexpected request for personal information.



Update your devices - Check that you have the latest software, apps, operating systems and security updates on ALL your devices. And update them regularly.



If it seems too good to be true, it probably is - It may seem tempting to click on a link - especially if it sounds like a good offer on Facebook - but it could be a phishing email.



Just take a breath - Don't rush in and hand over bank details or personal information. Do not reveal your passwords. Banks will never ask for your full password or pin. Neither will they or the police ask you to withdraw money or transfer it to another account

Taking a moment to think over what you're being asked for can stop fraud.

If you think you have fallen victim to a scam contact your bank immediately and report it to **Action Fraud** (National Fraud and Cyber Crime Reporting Centre) - 0300 123 2040. Report suspicious texts by forwarding the original message to 7726 which spells SPAM on your keypad.

For further information go to sharechecklist.gov.uk

Published: May 2021