FxPro
Trade Like a Pro

FxProtection & Online Security

Online scams and fraudsters have always been around but are prevalent now more than ever due to the ever-increasing digital world that we live in.

At FxPro we take all the necessary steps to protect our clients' information, however, you also need to ensure you are taking all reasonable precautions to prevent yourself from falling victim to online scams and make it harder for criminals to access your personal information.

Here are some top tips for protecting your online data:

Expect to be targeted

The biggest mistake people make is assuming that online fraud is rare and that they are unlikely to be affected. This is a false presumption; everyone and anyone can be a target. Always be suspicious and approach any unsolicited contact with extreme caution. Ignorance isn't bliss, its an invite to scammers.

Don't be duped into divulging your data!

Never disclose sensitive information such as passwords, account details, accounting information or identity details etc to anyone, even if they report to be from a reputable company. Only open attachments from trusted sources and never click on any email links or respond to requests for information, without verifying the legitimacy.

Understand the weapons used

Fraudsters often target individuals and organisations through phishing emails, phone & SMS spoofing etc. Watch out for scammers using similarly named email domains or social media accounts to appear as if the communication is from an official source. Even a phonecall/SMS from a number you know is not necessarily legit, as hackers can easily spoof numbers.

Protect your devices

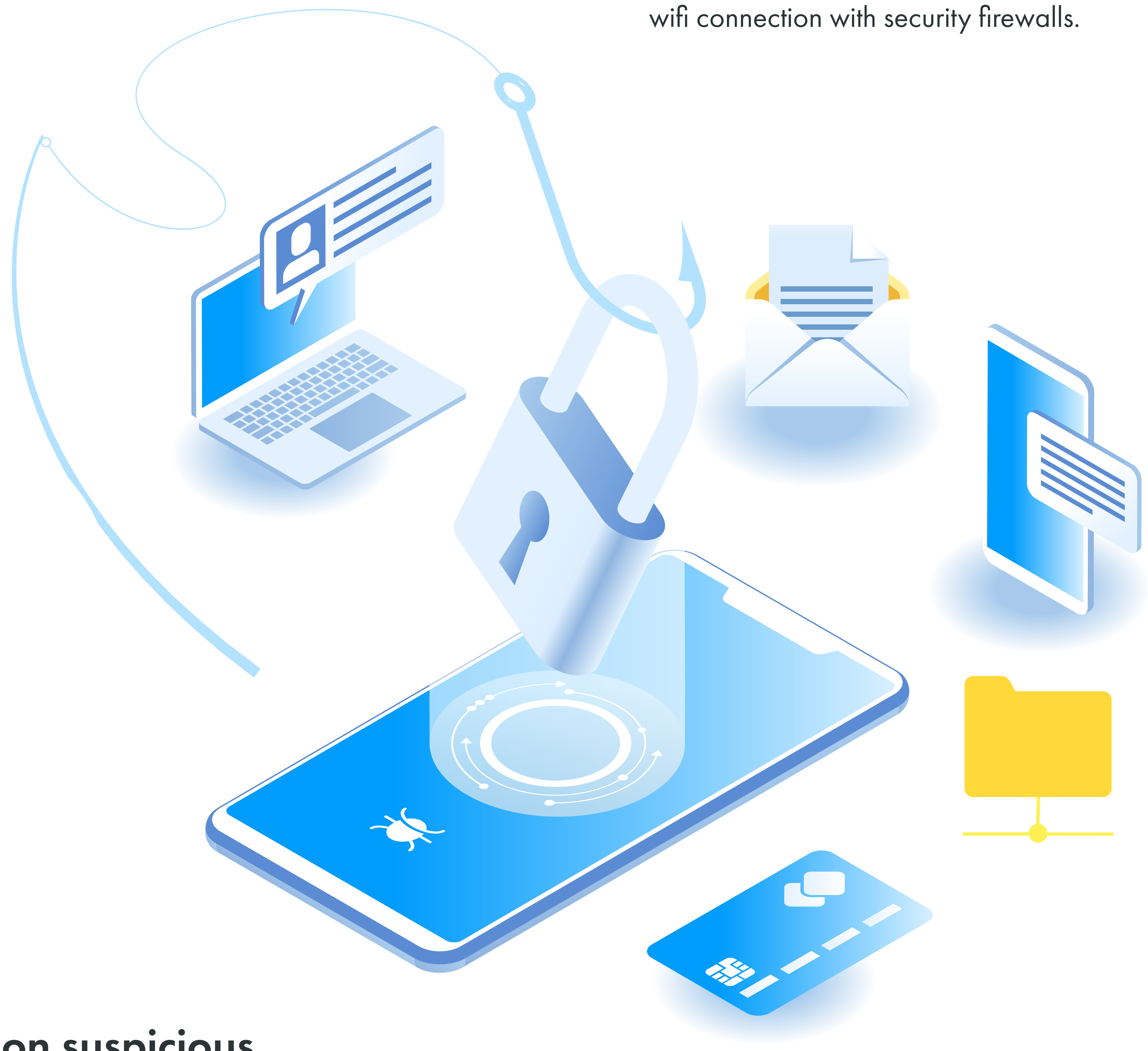
Install antivirus/malware software to any device you use and regularly scan for viruses. Never install programs/files from unknown sources; malicious malware and viruses can send information from your device or change transaction details in an attempt to steal your identity or funds. Likewise, never allow remote access to your device and always lock them when unattended.

Save details for next time? No thanks!

Never save payment details or login details online. It may seem tedious to manually enter each time, but it is not worth the stress and hassle of your card details being used or unauthorised access to your accounts.

Use a secure network connection

Don’t use public networks as they are easily hackable and often lack security. Ensure that browser/PC security settings are enabled and updated and only use a secure wifi connection with security firewalls.



Question suspicious or unsolicited contact

If you are not sure if the correspondence is legitimate, don’t be afraid to contact the company/bank/institution directly for confirmation through their official communication channels. They should be happy to address any concerns you have and may be able to assist you on what actions to take if your details have been compromised.

Browse Securely

Ensure that website where information is entered is using HTTPS protocols and shows the padlock icon in the URL bar. Pay attention to websites starting http:// and never enter any personal details or submit any forms through them, as it is easy for hackers to steal your information.

Password Precautions

Regularly change your password(s) using complex combinations and enable 2-step/multi-factor authentication wherever possible. Don't use passwords that contain family names, pets, nicknames, or well-known phrases/sports teams etc, as these are easily guessable. Also, use a different password for different sources or it only takes one hack to gain access to everything. Password hacking is one of the easiest ways for fraudsters to access your personal information without you even knowing.

Socially shield

Be careful what you share online, even in social media. Scammers or Identify thieves can find out a lot about you from details you post, making it easier to access your information or fraudulently impersonate you. Think twice next time you post and ensure that you are not unintentionally revealing private info. The same goes for messaging apps and chat rooms etc, you may know who you are communicating with but you don't know who else is watching or what their intentions may be.

Don't neglect email security!

Your emails may contain a lot of valuable info for hackers and once access is gained, they can then reset passwords, change account information etc. Frequently update your email password, enable MFA and never keep any personal documentation in your history. For example, if you have emailed someone your documentation in the past, a hacker can easily access these attachments and now have your Identity. If you ever see unauthorised access to any online accounts, the first action should be to ensure that your email has not been compromised.

For additional safety tips, what to do if you receive unsolicited contact or if your account has been compromised, please refer to our online safety page:

https://www.fxpro.com/safety

Be aware & stay safe online! If you have any questions at all or would like to verify any communication, please contact us via our official communication channels

support@fxpro.com
https://www.fxpro.com/contact us
+44 (0) 203 151 5550