



Guide to Staying Safe Online



Online Security at HiFX:

We want to make sure access to your account online is safe and secure. Here are some simple tips to stay safe online.

- Your client number, username and password are the key to your online account. They should never be given to anyone else and you should not write your password down anywhere. Change your password regularly to keep it safe
- Never give out your password. HiFX will NEVER ask you to supply your complete password; we only ever ask for random characters
- Be on your guard for fraudulent (or 'phishing') emails that claim to be from HiFX and ask you for your personal information or HiFX Online sign in details. We will never ask you for security details by email
- To be certain, it is a good idea to save <https://www.hifxonline.com.au/> into your 'favourites' and access it this way rather than clicking through to it from emails. This is a good practice to follow for all websites that you have security details for
- When visiting HiFX Online, always check for 'https' in the address bar and the 'padlock icon'. HiFX Online use SSL certificates provided by VeriSign. This is the same technology used by the world's 40 largest banks. Without SSL encryption, packets of information travel through networks in full view. Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it

Staying Safe Online:

There are some other simple actions you can take when online to better protect yourself:

- Check the security of e-commerce sites. Keep your identity secure. Counterfeit (or spoof) sites are often used by fraudsters to lull you into a false sense of security. Following these steps should ensure that the site you think you are using is a genuine secure site
- Check for 'https' and the padlock. Genuine secure sites have addresses that start with 'https' and display a padlock icon either beside or as part of the address bar or in the bottom section of your internet browser
- Double click the padlock. Double clicking the padlock icon that appears in your internet browser brings up information about the lock that can help you confirm that the site is genuine. If the lock is not within its valid dates or has been issued to a website that you do not recognise, do not enter your security details
- Use strong passwords. A good password should be longer than seven characters and contain a mix of letters and numbers. You should also avoid using your name, username or something too obvious as a password. Remember to use different passwords for logging into different sites and you should change your passwords regularly

What is Phishing?:

Phishing is a technique commonly used by fraudsters in an attempt to acquire sensitive information, such as usernames and passwords.

Here is how a phishing scam typically works:

The fraudster sends out a fake email that has been designed to look like it comes from a reputable source (like HiFX). This fake email asks for security details or directs customers to a counterfeit banking or commerce site. At the counterfeit site, the fraudster asks the customer to enter their complete security details - password, security questions and so on. These stolen security details are then used to commit fraud.

If you receive an email requesting your security details do not reply and do not follow the instructions even if the email suggests that you need to take immediate action to stop your account being frozen or it indicates that you may incur a fine if you don't. These are just tricks that the fraudster is using to manipulate you in to giving away your vital details.

If you are sent an email that requests you to enter your FULL password details it is NOT from HiFX.

If the email contains a link, once you have clicked through, check the URL on any pages asking you to provide your log in/ security details starts with <https://www.hifxonline.com.au> and look for the padlock symbol which represents a secure and encrypted connection to our web server.

What action should I take if I suspect I have received a phishing email?

If you've received an email, purporting to be from HiFX, that you believe may be fraudulent, please send the email to phishing@hifx.com.au This will allow us to investigate and help prevent further instances of phishing.

What should I do if I believe someone might have obtained my security credentials?

Please call us on +61 (2) 8270 4500. You should also change the password on your account immediately (ensuring that you access <https://www.hifxonline.com.au> and NOT via the suspect email).

Keep Yourself Secure:

There are also other steps you can take to keep your PC secure, including:

- Install and maintain anti-virus software
- Maintain a firewall on your PC to protect it from unauthorised access
- Always use the latest version of your web browser (e.g. Internet Explorer, Firefox). Web browsers often provide a level of inbuilt protection such as anti-virus and anti spyware. Using an out of date browser increases the likelihood that someone might be able to exploit a weakness, so having the most up to date version and ensuring that all security patches have been applied is important
- Look out for SSL Certificates (the https in the address bar) to verify you are visiting a trusted site and that your information will be encrypted for your security



- Always logout of secure sites. Never leave your computer unattended when logged in to a secure site and ensure that you log out properly when you have finished your session
- Be extra careful when using computers in public places. As you cannot be certain about the security of public wireless networks or computers in public places (like an internet cafe or library) you should be cautious about using some online services in these situations. Never change your security details while using a public wireless network or a public computer
- For more information you can also check websites such as Getsafeonline.org to keep up to date with the latest phishing or scam emails going around