Stay Cyber Safe

Cyber fraud is a real threat to your house move. We take this very seriously and will work with you to ensure that together we minimise the risks. But we need your help.

There are some easy ways to stay safe during your transaction with APL:

1. Our Bank Details

We have no plans to change our bank, so please ignore any email suggesting we have or might be doing this and call us immediately.

If you are in any doubt about our bank details there are several products online where you can verify them, e.g. the SafeMove Scheme, details of which are available at www.safemovescheme.co.uk/home/safebuyerproduct. Other products are coming to the market all the time.

2. Sign up to use our Secure Communications Portal

To provide maximum protection we maintain a secure online portal. Please use the portal for all communications as this will keep your data and money safe from criminals.

3. Never email sensitive data

If you need to share sensitive information about your transaction with us please supply the information by post or where appropriate over the phone. Never put this information in an email it is not a safe means of communication. You never know who is viewing or monitoring your emails.

Other ways to stay safe are:

1. Always lock your unattended devices

If you leave your computer, phone, tablet or external hard/flash drive unattended for any length of time lock it so no one can use it whilst you're away.

2. Implement good password management practices

- Change your password every 30 days.
- Use different passwords for each site you log into, especially your banking and shopping addresses.
- Use a selection of numbers, letters, upper and lower case and punctuation marks in your password.
- Never write your password down or share it with anyone.

3. Think before you click on attachments or links in an email

If you are not expecting the email or are suspicious for any reason, don't click on the attachment or link. Go to the website via a search engine or by typing in the web address if you know it. If you must click on the URL check it does not contain any spelling errors before clicking on it. A genuine URL will not contain spelling mistakes.

4. Keep your antivirus and malware software up to date

Ensure you update your security software on all devices e.g. Laptops, smart phones, tablets, kindles etc. when prompted and use a trusted security provider.

Check before plugging a new device into your computer as malware can be spread via infected flash drives, external hard drives and smartphones

5. Only do sensitive browsing on your own device or a trusted network

Never access or divulge your bank or card details via a device or network you don't own or trust. If you use a friend's phone, public computer or free WiFi you are at significant risk.

6. Be cautious about sharing personal information on social networks

Social media contains lots of information about you, your family, job, location, whether you are on holiday or moving house etc. Criminals use this information to access data that they then use to help them gain access to more valuable data about you.

Avoid posting updates about your sale or purchase online. This may help criminals to anticipate and track the transfer of funds which they will try to intercept.

7. Monitor your accounts

Keep an eye on your bank and credit card accounts etc. for any signs that your accounts have been compromised. Don't ignore an unfamiliar entry, report it to your bank and change your passwords.

8. Beware of downloads

When downloading apps to your mobile device always use a trusted source and trusted developer as mobile malware is the fastest growing risk.

Beware of messages and pop-ups that appear to be genuine programmes asking you to update your PCs antivirus or clean your system. Criminals use these to infect your PC and extort money from you. If you get a message saying your PC is infected never click on it.

9. Be careful what you browse

Criminals use popular events to disguise their activities and introduce malware onto your devices by creating what appear to be genuine sites covering the event. Search engines are aware of this practice and remove these sites from their search results but it may take some time to discover them

10. Offline security

Beware of calls or emails asking you for sensitive data. If you have concerns, call the company on a different phone first to verify the call or email is genuine before giving out your details.

Cybercrime Terminology

Phishing: a method used by criminals to access valuable online personal data e.g. usernames and passwords.

Vishing: a telephone call where the caller tries to obtain information about you which can then be used for identity theft.

Malware: software designed to access or damage your computer without your knowledge.

Man in the Middle: software that impersonating the connection between your device and a website so that information can be obtained about you and the third party you are communicating with.

Drive-by Downloads: where malware is downloaded to your device by visiting a genuine website that has been infected.

Spyware: a programme that secretly records what you do on your computer.

Botnet: computers that unbeknown to their owners are set up to forward transmissions to other computers on the internet.

Denial of Service Attack: high volumes of data or traffic are sent through a network disrupting service until the network can no longer function.

Malvertising: clicking on an infected advert which downloads malicious code to your device.