# Rules for the Safe Use of Web-Based Instruments
# Amore Finance

## Recommendations for Clients

### 1. Your login details are known only to you and to no-one else

Never disclose to anyone your login details for the web-based payment instrument (hereinafter the "*Internet Banking*"), especially your user number, login name, password, PIN and authorization code, and do not send these details by e-mail or via social networking sites. In particular, guard your privacy when logging in and make sure that no-one else can register your login details. Also, do not leave your computer or mobile phone unattended and use keyboard locks and device access codes. Refrain from using the Internet Banking products in public (e.g. in means of transport) or in rooms under surveillance (e.g. within the range of security cameras).

### 2. Check the device from which you access the Internet Banking

Do not use the Internet Banking on computers where you cannot be sure that they do not have any harmful programs installed. Make sure to avoid any public computers at Internet cafés or at airports or info centres. If possible, when accessing the Internet Banking, use only your personal computer or telephone. Always check in your web browser address bar that you are accessing the Internet Banking via a secure connection. You can check this simply by verifying that the address starts with https:// (the "**s**" at the end is what is important here) or you will be alerted to this by the web browser with green colour or with a padlock symbol in front of the website address.

### 3. Beware of unknown links and websites

Visit only well-known and credible websites. Today's attackers are resourceful and they can create a genuinely-looking reproduction of the login page of the Internet Banking and smartly navigate you to it. Therefore, beware of any unknown links both on the Internet and in your e-mail box that direct you to any pages resembling the login form of the Internet Banking, e-mail box or e.g. social networking sites. If the login screen of any Internet Banking product appears suspicious to you, do not log in. Always check the web browser address bar to make sure that you are really located on the website concerned and not on a fake one.

Especially dangerous are websites with erotic content or those for downloading software, videos and music which often contain plenty of dangerous software and viruses.

### 4. A suspicious e-mail? Do not open it and delete it

The Company will never send you e-mails requesting the disclosure of your identification details, user number, login name, password, PIN, authorization code, credit card details, etc. Please never respond to any such requests. In your e-mail box, open only trustworthy e-mails from well-known and expected senders. If an e-mail appears suspicious, you had better instantly delete it. If you have already opened it, make sure not to open any attachments or links it contains. And if you accidentally click on a link or open an attachment, then close it quickly to prevent the program or browser from installing any application. Subsequently, we recommend scanning the computer or mobile device with antivirus software.

### 5. Stay protected against spam

The best tool for eliminating most of the unwanted and hazardous mail is to set up and actively use e-mail protection against spam. Most public services offer this protection as do many e-mail clients such as Outlook and others. The setting of this protection is often intuitive and easy. Also consider using additional security applications such as antispyware and antiadware which will protect you from unwanted ads and harmful programs.

### 6. Use and update your antivirus program and firewall both in your computer and telephone

Perform regular checks of your devices by using your antivirus program. Never disable your antivirus program, don’t forget to perform regular updates (it is possible to set up automatic updates via the Internet) and use its latest version with implemented protection and malicious software detectors. Fraudsters never sleep and so the older an antivirus program is, the less effective will it be against new threats. We also recommend using a firewall on your computer. Install an antivirus program also on your smartphone. The belief that telephones cannot be attacked by viruses is a dangerous myth which may easily backfire against you. If you have a suspicion that your computer or mobile phone has been infested with a virus, do not use the device for accessing the Internet Banking or for any other services with your personal data (e-mail, social networking sites, online shops, etc.) and contact an IT expert.

### 7. Update your devices, computer and mobile phone

Also perform regular updates of your programs and operating system. It is especially important to update the Web browser in your computer and telephone and all its plugins (e.g. Flash Player). Also update all your security programs. Also check the releases of operating system patches and do not postpone their installation until the next time. For smartphones and tablets we recommend using the latest version of the operating system (firmware) which is officially offered by the device manufacturer. Any older version of your programs poses a potential threat to safe browsing or to your finances. Never install in your computer or telephone any programs of unknown origin. As for mobile phones, install only applications from official application stores – Google Play (Android), App Store (iOS), Windows Marketplace (Windows Phone).

### 8. Monitor your balance and transactions and report any inconsistencies to the Company

The best early warning tool to find out that anything is wrong is to know the balance in your account and the transactions you have made. If you register any operation you have not performed or if you have doubts about the accuracy of the balance in your account, please immediately contact the Company by telephone or e-mail. Do not postpone the reporting! Only a rapid response can prevent any further damage or help find a quick solution to a potential error.

## 9. Regularly check for news on Internet security

The more information you have, the safer your Internet behaviour can be. Therefore, regularly check for news on Internet security and observe all recommendations.