SOCIETE GENERALE

SOCIÉTÉ GÉNÉRALE SECURITY GUIDELINES

A. Protect your Connection to the Website:

- Use the correct URL to connect to the Website
- Keep your password confidential at all times and do not divulge it to anyone.
- Destroy any communication in relation to your password immediately after reading it
- Change your password after first connection to the Website
- Ensure you do not allow anyone (without exception) to use your login and password
- Choose a password that is hard to guess and do not use your login or personal information such as your telephone number, birth date or the like, to build your password.
- Avoid using an old password as a new password. Someone or a system may have kept traces of your old passwords
- The same password should not be used for different websites, online services, particularly when they relate to financial services
- Writing your password somewhere is like sharing your password : no one has to know your password (not even IT people)
- Change your password regularly
- If you suspect your password has been compromised notify SG immediately
- Do not leave your Terminal unattended when your are connected to the Website
- Quit the Website properly by using the log-out feature, and avoid just closing your browser
- Inform us immediately on the loss of your mobile phone(s) or change in your mobile phone number(s)

B. Other Security Requirements and Best Practices

Terminal

- Anti-virus, anti-spy ware and other internet security software must be installed on your Terminal and kept up-to-date.
- Ensure that your Terminal's operating system and software are regularly updated with the latest security updates and patches
- Ensure that access to your Terminal is protected with pin codes and/or other protection locks
- Do not install or run software of unknown origin
- Remove file and printer sharing on your Terminals
- Log off or turn off your Terminal when not in use
- Prevent unauthorized people from using your workstation
- Do not use a Terminal which cannot be trusted
- Check your last log-in date and time to the Website on a regular basis

Internet

- Always use the last version of your browser
- Make sure your browser is configured to the strongest security settings
- Do not select the browser option for storing or retaining user name and password
- Clear regularly your browser's cache
  Access Web sites by typing the Web addresses directly into your Web browser or by using Web addresses you have bookmarked, instead of via embedded links in unsolicited e-mails. **Please note that any access to SG Markets will be in the format of *.sgmarkets.com and that any other format received should be considered as fake.**
- SG Employees will never request your password or second authentication factor directly through emails chat or phone calls
- All links in security related email sent by SG Markets will lead to sgmarkets.com or its subdomains
- When connecting to financial online services, check that the financial institution's website address changes from http:// to https:// and a security icon that looks like a lock or key appears when authentication and encryption is expected.
- Terminate a log-in session if an SSL certificate does not belong to Société Générale and a warning is given to this effect. Inform us immediately of such warning message.
- Do not disclose personal or financial information in forum, chats, or suspect websites
- Avoid using financial online services on public computers (Cyber cafés, etc)

E-mails

- Be vigilant with an e-mail from unknown sender or suspicious e-mails: do not open attachments, do not click on internet links, regardless of how enticing it may be
  - Do not communicate your credentials by e-mail
  - Delete junk or chain e-mails

Data Protection

- Regularly backup your critical data
- Use encryption technology to protect highly sensitive data

Accounts

- Check your account statements, including account information, balance and transactions, on a regular basis and report to us any discrepancy

C. Common Threats

Viruses are not the only threats when using computers. Cybercrime is growing as well as the number of threats. When dealing with financial online services, it is important to be aware of these threats, especially Social Engineering and Phishing

Social Engineering

Definition

The Social Engineering describes any effort to manipulate you into giving up confidential information. The attacker using social engineering usually poses as a legitimate person in the organization and tricks computer users into giving useful information. This is usually done by telephone, but it may also be done by forged e-mail messages or even an in-person visit. These scams can put your identity or computer security at risk.

Protect Against Social Engineering

If you cannot personally identify a caller who asks for personal information about you or anyone else (including badge number or employee number), for information about your computer system, or for any other sensitive information, do not provide the information. Insist on verifying the caller's identity by calling them back at their proper telephone number as listed in your organization's telephone directory. This procedure creates minimal inconvenience to legitimate activity when compared with the scope of potential losses. Verify the legitimacy of the request: Ensure that fulfillment of the request is within your domain of responsibility, do not be intimidated by someone pretending to be a VIP or a technical person needing urgent information, etc.

Phishing

Definition

Phishing attacks use 'spoofed' e-mails or SMS etc and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. The attacker using phishing usually send e-mails pretending to be a bank or a financial institution, etc., encouraging the recipients to connect to a fraudulent website disguised as the official website of this institution.

Protect Against Phishing

Be suspicious of any e-mail or SMS etc. with urgent requests for personal financial information. Check carefully the identity of the sender as well as the Internet address of the target website (e.g. https://www.sg.markets.com instead of https://www.sgmarkets.com)

Never click on the links in an e-mail to get to any web page, if you have doubts regarding the message authenticity. Avoid filling out forms in e-mail messages that ask for personal financial information. Always ensure that you're using a secure website when submitting sensitive information via your Web browser.