

Introduction

This brochure is intended to provide an explanation of some of the common forms of Internet fraud and provide some recommendations on how to protect yourself. Please keep in mind that Security is not complete without U.

Forms of Internet Fraud

Spam is unsolicited commercial email, electronic equivalent of the junk mail that comes through your letterbox. Spam can be used to direct users to a non-legitimate website, to "phish" the user in order to steal personal information such as credit card information. Spam can also direct the user to infect its personal computer with malware (i.e. harmful software) including viruses, trojans, worms and spyware.

Phishing uses social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by email, masquerading as a bank or trustworthy individual. Typically, you receive an email that appears to come from a reputable organisation, such as a bank. The email includes what appears to be a link to the APS Bank's website. However, if you follow the link, you are connected to a replica of the website. Any details you enter, such as account number, PINs or passwords, will be stolen and used by the hackers who created the bogus site.

Phishing emails give themselves away by telling you that there is some reason why you must provide personal details such as your APS 365 ONLINE logon, password, credit/debit card number or PIN by reply email or through a website. Phishing emails may seem plausible when first read and attempt to force the recipient to urgently reply or logon to a website before they have time to think about what they are doing.

Non-legitimate/Replica Websites are websites (URLs) you are directed to by phishing emails. These websites appear authentic but are, in fact, the mechanism for capturing your personal details. Often, these sites will not address you by name but by general names such as Dear Client or Dear Customer, will contain incorrect grammar or spelling, and will not have an authenticate certificate. However this does not mean that this is a 100% fail-safe method of how one can detect such as emails. It is important to note that APS Bank will never ask you for personal details by emails, mails or telephone calls including passwords, User -IDs, PINS, address and accounts number.

Viruses are programs developed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. In addition, many viruses are bug-ridden and these bugs may lead to system crashes, data loss and stealing of data. A computer virus passes from a computer to another. A computer virus must piggyback on top of some other programs or document in order to get executed. You might receive an infected file in a variety of ways, including via an email attachment, in a download from the internet or on a infected portable media such as portable USB drives, diskette, CDs and DVDs.

Worms is a computer program that has the ability to copy itself from machine to machine. Worms normally move around and infect other machines and do not need a program. They infect other machines through computer networks. It is important to be extra cautious when visiting strange sites or when chatting with your friends.

Trojans are programmes that enter your computer undetected, giving the intruder unrestricted access to the data store on your computer. Trojans can transmit personal information including card information and other confidential data even if you are not accessing that data at the time. Trojans can be sent either as an email, spam mail, an attachment, or embedded in a web page. It is recommended to log-off from a website and to use the 'File Close' instruction rather than click on the 'X' in the upper right corner of the screen.

Spyware is spy software that enables intruders or advertisers to gather information without your knowledge. You can get spyware on your computer when you visit certain websites or a popup message may prompt you to download a software utility or the software may be downloaded without your permission.

In order to mitigate the risks from such threats a suitable auto-update anti-virus and anti-spyware should be installed. You should always be extra cautious when surfing the Internet. APS Bank will never ask for personal information through emails, telephone or SMSs.

Protect yourself on the Internet

Secure Your System

- Use and maintain a good auto-update anti-virus.
- Use and maintain a good auto-update anti-spyware.
- Use a personal firewall.
- Always use original licensed software and operating system.
- Always download and install authorised operating system updates. Do not run or install programmes of unknown origin.
- Do not access your bank account(s) from public computers such as Internet cafes or Hotels.
- Always log-off properly from APS 365 ONLINE Internet Banking before leaving your PC unattended.

Password Guidelines

Avoid

- The use of repeated passwords or key close together on the keyboard.
- The use of repeated characters
- The use of names, themes, common words, family names, initials or private information that can reside in the Bank's database including address, ID Card, NO, Birthdays etc..
- The use of Bank name, identifiers or references
- The use of car registration numbers
- The use of months of the year, days of the week or other date criteria
- The use of word or number patterns
- The use of telephone numbers
- The use of user-id, username, group-id, answers to questions, token pins, token serial numbers or system identifier
- The use of words found in a dictionary (English, Maltese or foreign)
- The use of the above spelled backwards
- The use of the above preceded or followed by a digit
- The use of 'autocompletes', 'autosaves' or saves your password i.e. - do not tick the "remember this password" box

Do

- Make your password as long as possible.
- Use different types of characters even non-alphanumeric characters such as \$, # etc.
- Consider using a string of words, rather than a single word.
- If you suspect your passwords or pin has been compromised, change it as soon as possible and advise APS Bank.
- If you lost your token or mobile, advise APS Bank as soon as possible.

Best Practices

- Delete suspicious email(s) with attachments and never open the attachments.
- Delete without opening emails requesting personal details such as PINs or passwords - APS Bank will not ask you to provide personal details through emails, phone or SMSs.
- Check for secure connection and double click on the 'padlock' icon on the bottom right corner to show you who really own the certificate and that it is issued by a Trusted Certificate authority in this case Verisign.
- Type APS Bank's URL address yourself avoid using short-cuts and links from emails.
- Reconcile your account(s) either on-line or by statements frequently and regularly.
- Always check for announcements or security advertisements on APS Bank's website.

Report any suspicious activities

If you think that your PC has been compromised or you received a phishing scam, or that you may have received malware that enables someone to steal or access your account(s) details, lost your token or your mobile, report it immediately to the Bank.

Fraudulent Emails

Fraudulent Emails are emails that are being circulated purporting to be from a legitimate site. These emails request APS 365 ONLINE Internet Banking customers to go to a particular website and re-confirm their username, password or other personal information due to a security update, research or confirmation.

Please remember APS Bank NEVER asks customers for login details or personal information or account details through email or phone.

What should you do if you have received such emails claiming to come from APS Bank?

1. Do not click any links. Do not open any attachments. Do not enter any details.
2. Forward the email to 365online@apsbank.com.mt and then delete the email.
3. Contact the Customer Support Centre by telephone on 21226644

Security is Everyone's Responsibility

Internet Security

The Internet has changed the way financial institutions do business. Internet banking provides convenient access to information and the ability to perform transactions from home, work or other locations. An inadequately protected computer can be accessed by an unknown party or malware in a very short period of time. It is important to be aware that Internet is public and everyone can access it.

Guidelines to protect your computer and passwords

Protecting your passwords, tokens and mobile phones

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected.

Passwords can be in the form of a hardware token, token pins as well as mobile one time passwords. Passwords are an important aspect of computer security. They are the front line to ensure that only you are accessing your accounts and hence its importance to protect the passwords, token, token pins as well as your mobile phone.

It is your responsibility to ensure that your access to the APS 365 ONLINE Internet Banking facility is protected. It is very important that you adhere with the following security practices:

- Select a password that is easy for you to remember but difficult for others to guess.
- Do not select as part of your PIN your ATM 'key' or another already used password or number combinations that may be easily guessed, such as consecutive numbers (e.g. 7890) or use of same (e.g. 1233).
- Keep your password, token and token pin confidential and do not share it with anyone even to members of your family and APS staff.
- Do not write your password or token pin down or store it in a file on your computer or portable media such as USB, diskettes, DVDs, CD-ROMs and mobile phone handset.
- Always keep secure your token and mobile even from members of your family.
- Do not leave your token or mobile phone unattended at anytime.
- Never disclose your password or token pin in an email, voice or over the Internet.
- Ensure no one observes you typing in your password, PIN, your one-time password (OTP) including from cameras.
- Change your password on a regular basis at least once every three months.
- Change passwords and token that has, or might have been disclosed.
- Be aware that data sent through the Internet is generally unsecure and everyone can sniff the data.

Protecting your computer

APS Bank has provided a secure channel for the Clients to communicate with the Bank. Once the information has reached your computer, it's up to you to protect it. To protect the information, you should:

- Never leave your computer unattended while using the online internet banking services.
- Always exit the Internet Banking site using the logout button and close your browser if you step away from your computer.
- Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- Prevent the browser from caching (storing) the pages that you view by using the Enhanced Security feature located in the login screen.
- Secure or erase files stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to "empty" the cache.
- Disable automatic password-save features in the browsers and software you use to access Internet Banking.
- Use an auto-update anti-virus and anti-spam.
- Update and install new security patches as soon as they are available both for your operating system and Internet browser manufacturers make them available through internet. It is important to stay up to date with software patches.
- Block files with more than one file-type extension such as .JPG.VBS and .TXT.VBS. Such examples are ANNAKOURNIKOVA.JPG.VBS and LOVE-LETTER-FOR-YOU.TXT.VBS.
- Block file types that often carry viruses such as EXE, COM, PIF, SCR, VBS, SHS, and BAT file types.
- Never respond to emails, telephones or mails that ask you for your personal information including passwords, pin details etc, especially those that may seem to have been sent by APS Bank. Remember that APS Bank will never ask you for such personal information.
- Ensure that before using WI-FI adequate security must be enabled on your PC especially if you are accessing the Internet through a Hot Spot. Use WPA2 or better enhanced wireless technology.
- Remove or disable your wireless card if you are not planning to connect to a Hotspot Service or you don't need any network service.

Safety precautions to avoid the use of non-legitimate websites (Phishing/Pharming)

- Type in the Banks' websites by typing the full address into the address bar yourself. Don't follow links embedded in an unsolicited email or saved in favourites.
- Ensure that the Banks' page Internet banking web site will begin with 'https' to indicate that data is being sent secure.
- Bear in mind that this tells you that the website is using a secure channel, but doesn't necessarily mean that the website is legitimate.
- For Internet Banking purposes the Bank is using extended certificate to make it more difficult for phishers and counterfeiters to direct the client to another website. When clients visit the Bank's Internet Banking, the browser will trigger the address bar to turn green and display the name of the Bank listed in the certificate as well as the certificate's security vendor (VeriSign). This is possible only with the latest Internet Browsing technology.
- Keep a regular check at least once a week on your bank and card statement to ensure that all transactions are legitimate.
- Avoid the use of public computers/hotspots such as Internet Cafe', Hotel or Airport. Computers can have key loggers installed and they can steal your passwords. Besides computers will not be set as secure as they will be used by different customers and therefore different needs. There can also be nearby cameras which can be used for piggy-backing.