CMSGu2011-07

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Secure Internet Banking

CERT-MU

National Computer Board
Mauritius

Version 1.0

September 2011
Issue No. 7

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide guidance to users on the ways in which fraudsters operate and useful advice on how to better protect themselves when banking online.

1.2 Audience

This document, while generic in nature, provides the background information to understand the risks of Internet banking and the precautions to take in so doing. The intended audience for this document includes all individuals and organisations that make use of the Internet for any banking transactions, such as balance inquiries, money transfers and payments.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on Internet banking.

Section 3 provides the common online banking scams.

Section 4 discusses the online banking safety measures.

Section 5 concludes the document.

Section 6 comprises a list of references that have been used in this document.

2.0 Background on Internet Banking

Internet banking (or Online banking) enables customers to carry out financial transactions on a secure website operated by their retail or virtual bank**,** credit union or building society. Online banking solutions have many features and capabilities in common, but traditionally also have some that are application specific.

The common features generally fall under the following categories:

- Transactional (e.g., performing a financial transaction such as an account to account transfer, paying a bill, apply for a loan, new account, etc.)
    1. Payments to third parties, including bill payments and telegraphic transfers
    2. Funds transfers between a customer's own transactional account and savings accounts
    3. Investment purchase or sale
    4. Loan applications and transactions, such as repayments of enrollments
- Non-transactional (e.g., online statements, cheque links, chat)
    1. Viewing recent transactions
    2. Downloading bank statements, for example in PDF format
    3. Viewing images of paid cheques
- Financial Institution Administration
- Management of multiple users having varying levels of authority
- Transaction approval process
- Features commonly unique to Internet banking include personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

Although Internet banking is a very common way of accessing your bank account, it is vital to be aware of the ways in which criminals can try to gain access to your account and to learn how to protect yourself and your money.

Financial institutions that employ any form of Internet Banking should have effective and reliable methods of authenticating customers. An effective authentication system is necessary

in order to comply with requirements to preserve customer information to prevent money laundering, reduce fraud, restrain identity theft, and promote the legal enforceability of their electronic agreements and transactions.

The risks of doing business with unauthorised or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

3.0 Common Online Banking Scams

With the range of payments becoming ever greater over the world, everyone needs to be aware of the coherent steps that should be taken to minimise the chances of being an online fraud victim. Being a victim of fraud can cause stress and worry, so taking measures to protect yourself is essential. Below are some common online banking scams.

3.1 Phishing

This is the name given to e-mails that claim to be from your bank or other organisations but are actually sent to you by fraudsters. These e-mails typically urge you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify or update your personal security information but, by doing so, you are actually giving your information to the fraudster who has created the fake website. The fraudster then uses the details to access your online bank account and take your money. One easy way to spot phishing e-mails is that they are usually addressed to "Dear valued customer" instead of using your name. This is because phishing e-mails are usually sent out at random as the fraudsters only have limited information such as your e-mail address. In a similar scheme, called "Vishing," a person calls you and pretends to be a bank representative seeking to verify account information.

3.2 Pharming

Pharming is the installation of malicious code on your computer without any acknowledgement on your part. In one type of pharming attack, you open an e-mail, or an e-mail attachment, that installs malicious code on your computer. Later, you go to a fake web site that closely resembles your bank or financial institution. Any information you provide during a visit to the fake site is made available to malicious users. Both phishing and pharming share the one characteristic, they are created using technology, but, in order to be successful, they require your information. In phishing attacks you have to provide the information or visit links whereas with pharming, you have to open an e-mail, or e-mail attachment, to become a victim. You then visit a fake website and, without your knowledge, provide information that compromises your financial identity.

3.3 Malware

Malware (malicious software) is a computer virus that can be installed on your computer without your knowledge. It is capable of monitoring your PC activity, enabling fraudsters to capture your passwords and other personal information. To be a malware victim, you must be tricked into performing actions you would not normally do. You have to install the malware on your computer either by running a program or by visiting a website through e-mail or instant message link. Then, you are requested to send your bank login information. Your financial information will then be at risk only after you perform all these steps. To make sure you do not become a victim of malware, make sure you have up-to-date anti-virus and anti-spyware software installed.

3.4 Money Mules

Money mules are people who accept fraudulently obtained money into their account, and then withdraw the money and transfer it overseas to a fraudster. Money mules are often innocent people who have been deceived into helping criminals transfer funds abroad. Criminals offer prospective mules the chance to earn some easy money - concealing the fact that the work is illegal by advertising the job as a "shipping manager" or "sales manager" for an overseas company. However, money mules are liable for prosecution and anyone who thinks they may have been deceived by such a scam should contact the police immediately.

3.5 Identity Fraud

This fraud involves criminals obtaining key pieces of personal information that they use to pretend to be you. Criminals use these personal details to obtain financial services products in your name such as credit cards, loans, state benefits, and documents such as driving licences and passports. Alternatively criminals can use your personal information to gain access to your existing accounts.

4.0 Online Banking Safety Measures

Whatever you use the Internet for it is vital that you take a few basic steps to ensure that your computer is protected against the latest threats. Just as you protect your house with locks on windows and doors and maybe also a burglar alarm, it is essential that you protect your computer by using up-to-date anti-virus software, doing regular scans of your computer to check for viruses, installing a personal firewall as well as the latest security updates for your web browser and operating system. To help improve your security online follow the following precautions:

4.1 General Safety Precautions

4.1.1 Before you bank online

- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- Install anti-spyware software on your machine.
- Download (from the internet) the latest security updates, known as patches, for your browser and your operating system. Set your computer to automatically download these updates if possible.
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are not always activated by default.
- Keep your passwords and PINs secret - do not write them down or tell anyone what they are.

4.1.2 Whilst banking online

- Be wary of unsolicited e-mails or phone calls asking you to disclose any personal details or passwords. Your bank or the police would never contact you to ask you to disclose your PIN or your online banking password.
- Always access your internet banking site by typing the bank's address into your web browser.
- Never go to a website from a link in an e-mail and then enter personal details.
- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or unbroken key symbol in your browser window when accessing your bank site. The beginning of the bank's internet address will change from "http" to "https" when a secure connection is established.

- Do not be fooled by convincing e-mails offering you the chance to make easy money. If an offer looks too good to be true, it probably is.
- Never leave your computer unattended when logged in to your online account.
- When making a payment, always double check that you have entered the correct account number and sort code - if you enter incorrect details the payment will go to a different recipient and it may prove difficult to get the money back.

4.1.3 When you have finished banking online

- Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café.
- Check your bank statements regularly and thoroughly. If you notice anything irregular on your account, contact your back as soon as possible.

4.2 How To Keep Your Personal Information Secure?

- Do not let your cards or your card details out of sight when making a transaction.
- Do not keep your passwords, login details and PINs written down.
- Destroy, preferably shred, any documents or receipts that contain personal financial information when you dispose of them.
- Do not disclose PINs, login details or passwords in response to unsolicited emails claiming to be from your bank or police.
- When entering your PIN in a shop or a cash machine use your spare hand to shield the number from prying eyes or hidden cameras.
- Only divulge your card details in a telephone transaction when you have instigated the call and are familiar with the company.
- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- If you have registered your card for online protection via *"Verified by Visa"* and *"Mastercard SecureCode"* ensure your password is kept safe and secure.
- Use secure websites by ensuring that the security icon (locked padlock or unbroken key symbol) is showing in the bottom of your browser window.
- Access internet banking or shopping sites by typing the address into your web browser. Never go to websites from a link in an e-mail then enter personal details.

4.3 How To Avoid Identity Fraud?

Help keep your identity safe by following these common sense precautions:

- Always keep important personal documents, plastic cards and cheque books in a safe and secure place. Without access to this information a criminal will find it very difficult to pretend to be you.
- Do not share personal information unless you are entirely confident you know who you are dealing with.
- Store your statements, receipts and documents that contain information relating to your financial affairs safely and destroy or preferably shred them when you dispose of them.
- Carefully check bank and card statements, as soon as they arrive. If you find an unfamiliar transaction contact your Card Company or bank immediately.
- Be aware that your post is valuable information in the wrong hands. If you fail to receive a bank statement, card statement, utility bill or other financial information contact the supplier.
- Get your post redirected to your new address if you move house.

4.4 How To Securely Shop Online?

To minimise your chances of becoming a victim of fraud whilst shopping online, you should:

- Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your sight.
- Sign up to "*Verified by Visa"* or "*MasterCard SecureCode"* whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you from being a victim of online fraud.
- Only shop on secure sites. Before submitting card details ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer 7 or Firefox 2). The beginning of the online retailer's internet address will change from 'http' to 'https' when a connection is secure. In some new browsers, such as Internet Explorer 7 and Firefox 2, the address bar may also turn green to indicate that a site has an additional level of security.
- Never disclose your PIN to anyone and never send it over the internet.

- Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to roll back if problems arise, but having all the aforementioned information will help your card company take up your case if you subsequently have any difficulties.
- Ensure you are fully aware of any payment commitments you are entering into, including whether you are authorising a single payment or a series of payments.
- Consider using a separate credit card specifically for online transactions.

5.0 Conclusion

Internet banking has become a must a people's daily life due to its ease of access and transaction processing in a timely manner. However, many individuals or organisations are not vigilant enough and do not take appropriate safety precautions whilst online. Consequently, this leads to fraudsters capturing their personal information and performing all sorts of fraudulent transactions on the Internet. For this reason, users of Internet banking should ensure that they follow secure principles when giving away or accessing sensitive information.

6.0 References

- Federal Financial Institutions Examination Council: http://www.ffiec.gov
- Bank Safe Online: http://www.banksafeonline.org.uk
- Wikipedia: http://en.wikipedia.org
- US CERT: http://www.us-cert.gov