Ten Commandments to Safeguard Your Bank Account

Dinu Vincent
is an electronics and communication engineering graduate, currently working in the security operation centre of a leading private sector bank in India. He is a certified ethical hacker and holds a computer hacking forensic investigator certification

Ever since Adam and Eve sinned in the Garden of Eden, God's desire has been to restore the broken relationship between God and people. God made a covenant, which is a promise from God that can never be broken. The covenant states that God wants a relationship with the people, but in order to have this loving relationship, they have to turn away from their sin. This can also be interpreted as the act of avoiding mistakes. So if we avoid mistakes, the relationship will exist forever and we will live in prosperity.

In this digital age, money transfer is a matter of a few clicks. With this advantage, there are drawbacks that allow an innocent user to be tricked easily by a fraudster, thus resulting in easy money for the culprit. The few tips explained in this article will help you to stay alert against such practices, and stay in a good relationship with your bank.

Validate the URL

Manoj is an employee working in an information technology (IT) company and his salary account is with HOPE bank. He has to transfer some money to his friend. So he accesses the bank's Internet banking website. Since he frequently uses this facility, he feels something odd about the portal. He identifies that the uniform resource locator (URL) address is *www.internetbanking.h0pebank.com* instead of *www.internetbanking.hopebank.com* (0 instead of o).

Phishing websites are hoax websites that have the look and feel of a legitimate website. Hackers create phishing websites to collect information such as Internet banking credentials, card details, automated teller machine (ATM) pin numbers and personal details, so that they can make use of these to pilfer money from the victim's bank account.

Pharming is the technique to redirect traffic from a legitimate website to a fraudulent one by making use of the former's vulnerabilities in the DNS server, or by modifying the host file of the victim's PC. Web pages used for pharming attacks are the same as that of the genuine website, which makes it difficult to spot the difference.

One good way to get away from these fraudulent websites is to validate their URLs. Nowadays, almost all banking websites and Internet banking portals have EVSSL certificates. Have you ever noticed your browser's address bar turning to green colour while accessing your bank's website? This denotes that the URL is verified by a certificate authority (approved). Phishing sites will lack these certifications.

Enable second-factor authentication

The most practical way to strengthen authentication is to necessitate a second factor after the username/password stage. Since a password is something that a user knows, ensure that the user also has something that thwarts attackers who steal or gain access to passwords.

Traditional two-factor authentication (TFA) solutions use hardware tokens that

users carry on their key chains. These tokens generate one-time passwords (OTPs) for the second stage of the login process. However, hardware tokens are comparatively expensive, difficult to track and replace when broken, and the effort for distributing these is time consuming. Also, these are easy to lose and hard to use.

Banks have come up with several solutions for OTP generation such as short message service based, mobile application based, email based, software token based, interactive voice response (IVR) based solutions and so on.

Carry out up to date patching of machines, use antivirus

Do you know Zeus? I am not talking about the Greek god of the sky and thunder. Zeus is a banking Trojan that is being used to steal banking information by keystroke logging and form grabbing. Zeus's mobile variant called ZitMo is well-known to circumvent popular TFA schemes with security codes being provided via text messages.

SpyEye and Carber have developed their respective mobile counterparts. Dyre, which typically targets customers of large financial institutions, was recently used in a large-scale, credential-phishing campaign targeting international banks.

Each malware tries to evade detection by an antivirus. It intercepts keystrokes, browser data, stored files and basically everything to sneak into a banking account and initiate an illegal money transfer. It even tries to install mobile malware on a smartphone, which allows criminals to steal the OTP.

By regularly applying software patches and using an updated genuine antivirus solution, you can stay away from this malicious software to a good extent. In order to have a healthy PC, always ensure that cracked/pirated operating system/software are not installed. Always remember that nothing comes for free.

Do not trust open/free Wi-Fi

Do you pay your bills online while having pizza and enjoying free Wi-Fi at your favourite coffee shop? Better stop before you pay. Like a lion waiting for its prey, someone is waiting in that Wi-Fi network to steal your credit card information, Internet banking credentials and a lot more even before it reaches your bank.

Experts warn against making any financial transactions on public Wi-Fi. Some even advise against checking social networks or email accounts for the same reason, because too much information can be exposed to hackers that can allow them to gain control of bank accounts. Also, there are rogue hot spots that direct users to legitimate-looking websites that prompt them to provide banking credentials.

Do not click on links that offer billion-dollar prizes

Everyone is familiar with emails saying, "Your email address has been selected to claim the sum of US$ 500,000 in the 2015 European lottery." Expressions such as "your email address was selected" or "your address has won" are blabbermouth signs that the message is part of a scam. After all, you have not used your address to participate in a prize draw, have you? And if you have, it was unlikely to have been European lottery. Fraudsters obviously expect some recipients to suspect a scam and attempt to convince them otherwise.

Similarly, you may receive phishing messages promising a lottery win from Coca Cola, Google's anniversary winning notification, Yahoo lottery award international programme, Microsoft's award promotion and what not. Should you receive an email of this type, visit the specific company's official website; most likely you will find that the company is not actually holding a lottery of any kind. Google translate

service has made life much easier for online fraudsters as now they can send messages to users all over the world in various languages.

Do not trust customer service seeking banking credentials

A phishing mail is an email fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients. Voice phishing (vishing) is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from users with a financial motive. Some fraudsters use facilities like Voice over Internet Protocol, caller ID spoofing and automated systems (IVR).

Just like phishing, smishing uses mobile phone text messages to lure consumers. Often the text contains a URL or phone number. The phone number often has an automated voice response system. And again, just like phishing, the smishing message usually asks for your immediate attention. Do not respond to any such messages.

The questions you need to ask yourself are:

1. Do you know the sender of the email? If yes, still be cautious before clicking on a link. If no, do not click on any link.
2. Is there any attachment in the email? If yes, is it executable (a file with extensions like .exe, .bat,

.com, .vbs, .reg, .msi, .pif, .pl or .php)? If so, do not click on the attachment. Even if the file does not contain the above-mentioned extensions, be cautious about opening it.

3. Does the email request personal information? If so, do not reply.
4. Have you checked the link? Move mouse over the link and check the URL. Does it look legitimate or does it look like it will take you to a different website?

If you receive an email or phone call asking you to call, and you suspect it might be a fraudulent request, look up the organisation's customer service number and call that number rather than the number provided in the solicitation email or phone call.

Do not sow your card in every card slot

How many of you have given the entire money in your account to waiter as a tip? Confused? Card skimmers, in the form of a small gadget that can be attached to a pant's belt are available in the market. Always be careful when you give your card to the waiter along with the invoice, and never acquaint him or her with your pin number. Beware of the following:

1. Card skimmers who can capture card data and store or transmit it wirelessly

2. Fake PIN pads to capture PINs

3. Wire-tapping devices placed in between telephone lines to which point-of-sale terminals are connected to capture card data during a transaction

4. Skimming devices sited over card slots of an ATM

Introduction of global Europay, MasterCard and Visa cards, and second-factor authentication like Verified by Visa/MasterCard Secure Code rollout, have brought a great level of security for card transactions. Banks have provided easier methods for customers to block cards and get a confirmation to that effect after blocking the card.

Thumb rule. Always insist on the card to be used in your presence and keep your password a secret. Never entrust your debit/credit card with anyone. Always have your bank helpdesk number handy so that it can be reached for blocking your card immediately in required cases.

Do not let anyone speculate your password

Many of us fill the very important password space with our full name, date of birth, mobile number, partner's name and so on.

These are the details that you have populated in your social media profiles. And still you think that these are tough to guess! While in truth, these seemingly uncrackable passwords are commonly used for social media accounts, Internet banking, email accounts, e-wallets, etc. Always follow the thumb rule of using hard-to-guess passwords and change the same frequently.

Pattern passwords are present in mobile banking applications for making fund transfer simple and fast. Sometimes these patterns remain on your mobile screens, which result in a smudge attack.

Do not let your mobile phone be the tool to loot you

Cybercriminals use fake banking applications having the look and feel of legitimate banking apps to trick users. They also use other popular apps, such as utilities, chats, portals and security apps to rope users into their scams and steal their mobile banking credentials. These fake apps upload stolen user information such as mobile phone numbers, account details, login credentials and even text messages (OTPs) to the attackers' command and control servers. Some malwares/fake apps are delivered through text messages containing a link asking users to upgrade the bank's app or downloaded by other malware.

Always install applications from trusted sources. Your smartphone is powerful and, at the same time, vulnerable to viruses/malwares.

Do not give an opportunity to eavesdroppers

There can be a number of risks if you do not take proper care while using computers in Internet cafes and libraries. Avoid financial transactions that might reveal valuable passwords or personal information such as credit card numbers.

1. Check for hardware keyloggers.
2. If possible, use a trusted Web based spyware-detection program to scan for spyware before using an untrusted public computer.
3. While basic keyloggers do just that, for logging your keys you could use an on-screen/virtual keyboard.
4. If you have been using the Internet, ensure you use the browser tools to delete files and cookies and clear the browsing history.
5. Protect any passwords you are going to use by using the browser's Internet options menu. If in doubt, check the browser's Help option.
6. Consider changing any passwords you may have used on a public computer once you get back home.
7. Be on the lookout for shoulder surfers, that is, make sure that no one is watching over your shoulder while you enter your passwords.

I hope this article gives you at least a vague insight into the kinds of risks your bank accounts may be exposed to. While technological innovations have been a big boon to mankind in today's fast-paced life, it is always better to put in a little caution from your end to ensure that the same technology does not strike back at you. After all, it is your hard-earned money at stake. Protect it from, as I may put it, e-looters. Do contact your bank immediately if you suspect any fraudulent activity in your bank account. ●