CYBER CRIMES- HAPPENING MAINLY IN BANKING TRANSACTIONS

As auditors, we are seeing there is an increase in the cyber-crimes happening among our clients. Usually the computer is hacked or they get access to your email or internet accounts instruct you to transfer funds, as though they are your regular customers. The mistake of not verifying the source the clients have transferred money and later they found out that they have been cheated.

We would like to caution you and to prevent the fraud by alerting you to be cautious at all times. Most importantly, you must have noticed that banks would not use email for communication or for transferring of funds.

I would recommend you to observe the following precautions to avoid banking transactions crime-

1. Always enable for receiving SMS alerts for any transaction notifications
2. Whenever transferring huge amounts of money to any party, always first transfer a small token amount, get confirmation from the party then transfer the balance
3. Set up two step verification in the form of One Time Passwords/ token that keeps generating new and different passwords to be entered in the system.
4. Many banks have last login tracker/ activity tracker, keep a check on it frequently to detect any unwanted activities.
5. Don't leave the PC unattended after keying in information while transacting on the web site.
6. Don't select the option on browser that stores or retains user name and password
7. If you have several bank accounts, avoid using the same online banking password for all.
8. Avoid accessing the Internet banking channel at cyber cafes, which are prone to attacks by hackers. Also avoid locations that offer online connections through wireless networks (Wi-Fi), where privacy and security are minimal.
9. Don't open, run, install or use programmes or files obtained from a person or organization you do not know or from someone who is not a reputed vendor.
10. Don't fill out forms in e-mail messages that ask for personal financial information, like account or credit card numbers.
11. Check your bank's Internet policy.
12. Some banks have enhanced security features in Internet banking. For example, if the money that you want transferred to another account exceeds a particular sum, you will need to enter a specific password for high value deals to validate the transaction.
13. Always log out when you exit the online banking portal. Close the browser to ensure that your secure session is terminated. Never simply exit by closing the browser.
14. Install a personal firewall to help prevent hackers from gaining unauthorized access to your home computer, especially if you connect to the Internet through a cable or a DSL modem.
15. Turn off file sharing and network discovery when using a public wireless network.
16. Set an appropriate one time transfer limit and one day transfer limit according to the size of your transactions and requirements. Some banks have set a limit for transfers, accept the system and procedures followed by the bank.

General Things to be careful about-

1) Secure your computer

It is crucial to help prevent cybercrime to have reliable, secure and up-to-date Internet security software. At minimum, you should have anti-virus and anti-spyware, and a personal firewall installed on your computer.

2) Use Strong Passwords

Use different password and username combinations for different accounts and resist the temptation to write them down.

3) Secure your Mobile Devices

Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources.

4) Install the latest operating system updates

It is crucial to help prevent becoming a victim of cybercrime as well as for your Internet security and privacy that you keep your operating system up-to-date. Be sure to have it set to update automatically

5) Protect your data

Protect your data by using encryption for your most sensitive files such financial records and tax returns. It is also crucial that you regularly backup all your important data and store it in another location.

6) Secure your wireless (WiFi) network

Have strong passwords for your WiFi. Do not leave it open and without security.

7) Protect your identity online

When it comes to protecting your identity online it is better to be too cautious than not cautious enough. It is critical that you be cautious when giving out personal ID such as your name, address, phone number and/or financial information on the Internet. Be certain to make sure websites are secure when making online purchases, etc. This includes enabling your privacy settings when using/accessing social networking sites.

8) Avoid being scammed

Before clicking on a file of unknown origin or link always think. Never feel that you have to be pressured by any emails. Be sure to check the source of the email opening and especially before clicking on any links within the email. When in doubt, verify the source. Don’t ever reply to emails that ask you to confirm your username and/or password or verify your personal information. This very likely is a phishing scam.

9) Be wary of online offers that look too good to be true

Supposedly "free" software such as smilies or screen savers, secret investment tricks sure to make you untold fortunes, and contests that you're surprised to find out you "won" without even entering (imagine that?!?) are more often than not enticing hooks used by companies to grab your attention. While you may not monetarily pay directly for the software or service, this supposed "free" software or service you asked for may be anything but free, containing adware (advertising software) that tracks your online behavior and annoyingly displays advertisements that you do not want to see.

To claim your supposed contest winnings you might have to divulge your personal information or purchase something (that's really free, isn't it! not!).The old saying really rings through in this case; if the offer is too good to be true than it probably is. At the very least, before taking any action, ask for the opinion of a person you trust, read through all that fine print or, better yet, just simply ignore it. You may have to divulge personal information or purchase something else in order to claim your supposed content winnings. If an offer looks so good it's hard to believe, ask for someone else's opinion, read the fine print, or even better, simply ignore it.

10) Turn off your computer—With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.