

Customer Awareness Program

Cyber Security Department
(CSD-CAP)

Public



شركة ولاء للتأمين التعاوني
Walaa Cooperative Insurance Co.

Table of Contents

- 1.0 Overview..... 2**
- 2.0 Shopping Online Guidelines..... 2**
- 3.0 Best Practices for Online Protection 2**
- 4.0 Best Practice for Password Protection 3**
- 5.0 Best Practices for Operating System Protection..... 4**
- 6.0 Best Practice of Identity Theft Protection..... 4**
- 7.0 Best Practice of Identity/Insurance/Debit/Credit Cards Protection 4**
- 8.0 Summary..... 5**

Doc. No.: CSD-CAP	Customer Awareness Program	
Ver. No.: 1.0		
Ver. Date: 2019-03-30		

1.0 Overview

Although we protect our customers from identity theft and financial crimes, the customers should know how to protect their identity information by implementing security best practices when accessing online portal on their personal or business computers. We strive our best to educate customers and strengthen the customers' trust to their online transactions.

Below are our recommendations for awareness of online transactions on the following areas: Online shopping, online protection, password protection, operating system protection, identity theft protection, and Identity/Insurance/debit/credit cards protection. The purpose of these recommendations is to enhance the customers' trust and to guide customers into how to safeguard their confidential information from being a victim of identity theft, electronic fraud victim, and other common threats.

2.0 Shopping Online Guidelines

The Internet is the most convenient way to purchase from groceries to houses. The ease and selection that the Internet provides to shoppers has changed the face of retailing. You can go to the retailer's website to make a selection without leaving your chair. When shopping online, we recommend that customers following the guidelines:

- ◆ Learn as much as possible about the product and seller.
- ◆ Understand the retailers' refund policies.
- ◆ Choose a secure password to protect account information.
- ◆ Use a secure checkout and payment process.
- ◆ If an offer sounds highly suspicious or too good to be true, it probably is a scam.

3.0 Best Practices for Online Protection

Several researchers proposed the best practices for online protection. Here is a list of best practices:

- ◆ Reconcile your banking transactions daily and look for unusual small amounts such as penny transactions. This may be an indication that your account has been compromised and a fraudulent plan is in progress.
- ◆ Never access bank, brokerage, or other financial services information at internet cafes or public libraries. Unauthorized software may have been installed to trap account numbers and log on information leaving the person vulnerable to fraud.
- ◆ Immediately alert the banks of suspicious transactions. There is a limited recovery window for these transactions and immediate escalation may prevent or minimize further loss.
- ◆ Do not share your user ID or password with anyone.
- ◆ Wireless networks are discouraged. If you use a wireless network, it is suggested that you use password protection.
- ◆ Always sign out of secure areas of websites, where a user ID and password are required.
- ◆ Be cautious before sharing your email address with questionable websites, as this increases your risk of receiving fraudulent emails.
- ◆ Delete suspicious emails without opening them; never open attachments in suspicious emails.
- ◆ When your computer is not in use, shut it down or disconnect from the Internet.
- ◆ Never provide sensitive account information in response to unsolicited emails, websites, or pop-up windows.

Doc. No. : CSD-CAP	Customer Awareness Program	
Ver. No.: 1.0		
Ver. Date: 2019-03-30		

- ◆ Always review your monthly account statements carefully and investigate any unauthorized activity on your account.
- ◆ Practice safe internet use. Never click on pop-up messages or links to applications contained in emails. Try to get into the habit of manually going to links that are sent to you. It is estimated that over 80% of malware is obtained from clicking on pop-up ads.
- ◆ Be suspicious of emails claiming to be from financial institutions, government departments, or other agencies requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes and similar information.
- ◆ Use caution when opening attachments and ensure they were sent from a trusted source.
- ◆ Avoid downloading programs from unknown sources.
- ◆ Never give out any personal information including user names, passwords, national ID number, or date of birth.
- ◆ Do not use personal information for your user names or passwords, like your national ID number or date of birth.
- ◆ Block cookies on your Web browser. When you surf, hundreds of data points are being collected by the sites you visited. This data get mashed together to form an integral part of your “digital profile,” which is then sold without your consent to companies around the world. By blocking cookies, you’ll prevent some of the data collection about you.
- ◆ Do not provide your full birthdate on your social networking profiles. Identity thieves use birth dates as cornerstones of their craft. Try posting only the month and day, and leave off the year.
- ◆ Use multiple usernames and passwords. Keep your usernames and passwords for social networks, online banking, email, and online shopping all separate.
- ◆ Customers should be cautious while opening attached pictures via email as it may contain hidden and harmful executable files which will redirect them to the attacker's website.
- ◆ Online customers should not click onto the attached URL via email, but instead they should copy this URL, and paste it into the address bar to be sure that this is a legitimate website.

4.0 Best Practice for Password Protection

The following are some recommendation for password protection:

- ◆ Change passwords at least every 90 days.
- ◆ Create a strong password with at least 10 characters that includes a combination of mixed-case letters, numbers and special characters.
- ◆ Ensure that your account information and security responses are not written where they can be seen or accessed by others. If the information must be written down, it should be secured under lock and key when not being used.
- ◆ Never share your user ID or password with anyone for any reason.
- ◆ Secure your computer with a password-protected screensaver that has a timeout feature activated after no more than 15 minutes.
- ◆ Avoid using an automatic login feature that saves usernames and passwords for online transactions.
- ◆ Install password management applications to build a strong password, and store it in a secure database instead of putting it anywhere.

Doc. No. : CSD-CAP	Customer Awareness Program	
Ver. No.: 1.0		
Ver. Date: 2019-03-30		

- ◆ Some banks grant their customers a token for accessing their online transactions account to enhance the level of security. The user should wait until the code changes and then enter the new code displayed to ensure that the code has not been stolen.

5.0 Best Practices for Operating System Protection

The following are some recommendations for the protection of Operating Systems:

- ◆ Ensure that you use a current anti-virus and antispyware product to protect yourself against malicious software that is created for the specific purpose of gathering information such as user ID, passwords, and other critical information that may be stored on your computer.
- ◆ Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and to other computers.

6.0 Best Practice of Identity Theft Protection

The following are best practices for identity theft protection:

- ◆ Report lost or stolen identity ID or credit cards immediately.
- ◆ Never give out any personal information to anyone whose identity you can't verify Shred any documents you do not need that contains personal information such as bank statements, unused cheques, deposit slips, credit card statements, pay stubs, medical billings and invoices.
- ◆ Do not give any of your personal information to any websites that do not use encryption or other secure methods to protect it.

7.0 Best Practice of Identity/Insurance/Debit/Credit Cards Protection

The following are some recommendation for Identity/Insurance/Debit/ Credit Cards protection:

- ◆ You should never loan your cards to anyone.
- ◆ Carry only the cards you use frequently.
- ◆ Never leave your wallet or purse in your vehicle.
- ◆ Safeguard your ATM access cards and PIN as you would your cheque, deposit and money. Memorize your PIN – Do not write it on your card or in your cheque book.
- ◆ Consider using another machine or coming back later if you notice anything suspicious when using an ATM, stand squarely in front of the machine to keep your transaction as private as possible.
- ◆ Consider cancelling your transactions if pick-pocketing occurs or any suspicious activities you notice while using the ATM machine.
- ◆ Protect the sensitive magnetic stripe on the back of your card. Keep it away from direct sunlight. Avoid leaving your card on or near electrical appliances, such as the TV or stereo.
- ◆ Do not carry your card next to another card as they may demagnetize each other.
- ◆ Report all ATM crime-related activity to the owner/operator of the machine and to local law enforcement officials immediately.
- ◆ Always take your receipt with you at the conclusion of every transaction to assure your financial privacy. Keep your receipts and use them to check your monthly statement.

Doc. No. : CSD-CAP	Customer Awareness Program	
Ver. No.: 1.0		
Ver. Date: 2019-03-30		

8.0 Summary

How to Protect Yourself:

- ◆ Make sure your operating software, web browser or mobile apps are up-to-date.
- ◆ Install and regularly update a virus protection program.
- ◆ Scan your computer or mobile device for spyware regularly.
- ◆ Avoid downloading programs or apps from unknown sources.
- ◆ Do not share your user ID or password with anyone.
- ◆ Choose passwords with letters, numbers and special characters, and change your passwords often.
- ◆ Always sign out of secure areas of websites, such as Internet Banking, where a user ID and password are required.
- ◆ Be cautious before sharing your email address with questionable websites, as this increases your risk of receiving fraudulent emails.
- ◆ Delete suspicious emails without opening them; never open attachments in suspicious emails.
- ◆ When your computer is not in use, shut it down or disconnect from the Internet.
- ◆ Never provide sensitive account information in response to an unsolicited email, website, or pop-up window.
- ◆ Always review your monthly account statements carefully and investigate any unauthorized activity on your account.
