Online Banking Security Considerations

Online Banking is an easy, and secure way to do banking at your convenience. However, just as we take precautions with traditional banking, we also need to take precautions when using Online Banking.

What is Online Fraud?

When someone poses as a legitimate person or organization to obtain your information, and then fraudulently conducts transactions on your bank accounts, it is considered Online fraud. Common methods of Online fraud are fraudulent emails, websites, and pop-up windows, or any combination of these with other social engineering techniques.

What is Social engineering?

Social engineering is the manipulation of people, so they divulge confidential information. Criminals tricks a person into giving them User Ids, passwords, Credit Card numbers, or bank information; or accesses their computer and installs malicious software to gain this information, and to also control the computer.

What is Pretexting?

You receive a phone call from someone claiming to be from your financial institution. They speak to you about your accounts and personal information in a way that suggests they are legitimate. However, the person is an identity thief who has uncovered some information about you and is looking for more so they can attempt fraud.

What is Phishing?

Phishing is where a person is contacted by email, telephone or text message by someone posing as a legitimate person or organization, to lure that person into providing confidential information such as User Ids, passwords, Credit Card numbers, or bank information.

What is Pharming?

Pharming is the redirection of users from legitimate websites to fraudulent websites where confidential information such as User Ids, passwords, Credit Card numbers, or bank information are requested.

Security Controls

Cargills Bank Internet Banking has several fraud mitigant measures in place, including the following:

- Secure access and verifying user authenticity:

A unique User ID and Password combination is given for proper identification.

- Automatic Log Off / Session Time out

After 05 minutes of inactivity, your Cargills Bank Online Banking session will automatically log you off to avoid unauthorized access.

- Password Lockout

If your Password is entered incorrectly six times consecutively, you will be "locked out" of Online Banking until the bank can verify your identity.

- Secure Data Transfer / Encryption

Encryption of information is used within your Online Banking session.

Smart ways to Use Online Banking

You can play an important role in securing your Online Banking.

Password Protection

MAKE your Password safe

- Set a password that is difficult to guess for others. Use a combination of numbers, special characters, and upper and lower case letters (e.g. AzXd#185)
- Avoid using a number or name that is likely to be guessed by others. For example, avoid names and birthdates of family members.

- Avoid using the same Password for different accounts.

KEEP your Password safe

- Never disclose your Password to anyone. Keep your User ID and Password confidential at all times.
- Never write down or record a Password without disguising it.
- Never store your Password on computers, mobile phones, or placed in plain sight to others.

USE your Password safe

- Ensure that no one is watching you while you enter your Password.
- Never read out your Password over the phone.
- Never include your Password in an email.
- Never save your password in the web browser or mobile phone.

DON'T share an OTP

- An OTP will be sent only to your mobile number or email registered at Cargills Bank.
- Make sure you update your mobile number or email so you can receive your OTP.
- Do not share your OTP with anyone.

Secured Access

- Avoid accessing Online Banking via public computers, shared mobile or public Wi-Fi.
- Enter www.cargillsbank.com website address directly. Never access our website or provide your personal information (including your password) through any hyperlinks or attachments embedded in emails or from websites.
- Check the website URL to ensure it begins with a 'https' prefix. The common 'http' prefix (i.e. without the trailing 's') is not secure.
- Download mobile applications from reputable sources only, e.g. Apple App Store, Google Play.

- Always lock your mobile phone by a password or pattern when it is not in use.
- Do not leave your computer or mobile phone unattended when you are accessing your Online Banking.
- Remember to logout immediately after use. Closing the browser does not log you out. Click on the "Logout" button and follow the log out procedures to protect your account information.

Messages from bank

- Cargills Bank will never send an email message requesting confidential information such as account numbers, PIN Numbers or Passwords. If you receive such a request, contact Cargills Bank Customer Care on + 94 11 7640 640 immediately.
- You must provide a valid mobile phone and contact number for notification purpose. If any of these numbers is changed, please notify the Bank immediately.
- Check the SMS notification sent to you after each fund transfer.
- If you suspect someone has accessed your Online Banking or you have noticed suspicious transactions, immediately contact Cargills Bank on + 94 11 7640 640.
- If you have any suspicion or receive One-Time Password through SMS or email more than once, immediately contact Cargills Bank on + 94 11 7640 640.
- Check your accounts periodically and review alerts and statements.

E-mail Security

- Avoid opening suspicious emails requesting your account information and/or password, or mail from unknown senders. If you have opened any suspicious email, do not open any attachment or link it may contain. Delete the email.

Online Shopping Security

You can enjoy safe and convenient online shopping using your Card by following some simple rules:

- Only use “secure” web pages when you enter your Card details. A web page is secure if there is a locked padlock in the lower right-hand corner of your browser, or if the address starts with ‘https’, where the ‘s’ stands for secure.
- Practice safe computing (e.g. encryption, virus scanning software, firewall, anti-spyware software and similar safeguards).
- Use reputable Online stores. For example, check that the Online store has a return and refunds policy.
- If you have to use a password to access a service, make sure it isn’t easily identifiable and don’t disclose it to anyone.
- Don't save your passwords, Card Expiry info or CVV information on websites.
- **Be Smart;** if you see any unbelievable discount offer/ Deal, Clarify before making the payment.
- **Avoid Shopping in Public;** Use your own laptop or pc and avoid accessing shopping sites while sitting in a public café
- **Keep receipts**; Print Your Online Credit Card Receipts. When you use your credit card online, always print or screenshot a copy of your receipt or confirmation to track your spending details. Then, compare the amount on your receipt to the amount on your billing statement to make sure the totals match
- **Check SMS alerts & Statements regularly;** don’t wait for your bill to come at the end of the month. Use Online banking\ Mobile banking apps regularly, to view electronic statements for your credit card, debit card, and checking accounts.
- Contact Cargills Bank Customer Care on + 94 11 7640 640 immediately if an unrecognized charge appears on your Card statement.

Important Press Release from CBSL

press_20190801_adopting_safe_and_sesuring_the_Safety_o

press_20190206_En