CUSTOMER SECURITY AWARENESS FOR INTERNET BANKING

The banking industry has seen significant changes in the internet banking threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customersôonline accounts. Our Bank is providing security awareness information for your use and action to help protect your online account and transaction information.

Tips to Reduce the Risk in Internet Banking:

Secure Session: When banking on the internet, there are two simple indicators to confirm your session is secure: https:// in the URL, and a digital certificate (padlock or key) in the bottom right hand corner. If you do not see these, your session may not be secure.

Anti-Virus Protections: Make sure the anti-virus software on your computer or mobile device is current and scans your email as it is received.

Sign Off and Log Out: Always log off by following our secure exit procedures.

Block cookies on your Web browser: When you surf, hundreds of data points are being collected by the sites you visit. These data get mashed together to form an integral part of your õdigital profile,ò which is then sold without your consent to companies around the world. By blocking cookies, youôll prevent some of the data collection about you. Yes, youôll have to enter passwords more often, but itôs a smarter way to surf.

Don't put your full birth date on your social-networking profiles: Identity thieves use birth dates as cornerstones of their craft. If you want your friends to know your birthday, try just the month and day, and leave off the year.

Don't download Facebook apps from outside the United States: Apps on social networks can access huge amounts of personal information. Some unscrupulous or careless entities collect lots of data and then lose, abuse, or sell them. If the app maker is in the U.S., itôs probably safer, and at least you have recourse if something should ever go wrong.

Use multiple usernames and passwords: Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate. Having distinct passwords is not enough nowadays: if you have the same username across different Web sites, your entire romantic, personal, professional, and ecommerce life can be mapped and re-created with some simple algorithms.

Avoid Public Wireless Internet Access: You should be vigilant if you use internet cafes or a compute that is not your own and over which you have no control. Hackers and identity thieves often monitor these networks or install malware to capture your login credentials.

Protections and liabilities for business and consumer transactions using our secured internet banking:

To access our Internet Banking service, you must use the Access ID and Password you established when you activated your Internet Banking Customer Account. It is your responsibility to safeguard the ID and Password. Anyone to whom you give your Access ID and Password or other means of access will have full access to your accounts even if you attempt to limit that person's authority. You or someone you have authorized, by giving them your Access ID and Password or other means of access (even if that person exceeds your authority), can instruct us to perform the following transactions:

Make transfers between your qualifying accounts to the extent authorized;
Obtain information that we make available about your qualifying accounts;
Obtain other services or perform other transactions that we authorize.

You must have enough money in any account from which you instruct us to make a payment or transfer. You also agree to the Terms & Conditions of your deposit account that you received when you opened your deposit account.

Statements
Your Internet Banking payments and transfers will be indicated on the monthly or quarterly statements we provide. Please notify us promptly if you change your address or if you believe there are any errors or unauthorized transactions on any statement, or statement information.

If you are a a Business Online Plus customer we suggest you periodically evaluate the possible risks to your account. Some key areas to check are:

Who has access to the internet banking PC and credentials?
Is (Are) the internet banking PC or PCs secured after normal business hours?
Do you have up to date antivirus and antimalware software on the PC?
How often do you change the internet banking password and who knows the password?
Is there a firewall active on your PC?