How you can protect your online security

While UBS Financial Services Inc. seeks to protect your information on our systems, it is very important that you take precautions to protect yourself and the information you share over the Internet. You can use the following recommendations to protect yourself online.

Protecting your login information

Your user name and password are the keys to your access into Online Services. You should be careful in selecting and maintaining them to protect your information.

Your user name

Follow these tips when creating your own unique user name:

- Select a user name that you can easily remember
- Create a user name longer than the minimum requirements (longer user names are harder to guess).
- Do not select a user name that can be easily guessed by someone else.
- Memorize your user name and never write it down.
- Do not share or reveal your user name to anyone.

Tip: If you wish to use your name or something equally familiar, we suggest you mix numbers with letters to provide additional complexity.

Your password

Follow these tips when creating your own unique password:

- Memorize your password and never write it down.
- Regularly change your password. **This is a very effective way to increase your security.**
- Do not share or reveal your password to anyone. (Note: UBS Financial Services Inc. will never ask you for your password.)
- Select a password that cannot be easily guessed by someone else.
- Do not associate your password with anything personal such as names, birth dates, phone numbers, or other familiar words.
- Create a password longer than the minimum requirements (longer passwords are harder to guess) .

Additional security measures

- Remember to log off of Online Services when you finish your session. UBS Online Services provides a "Log out" button in the upper right-hand corner of your screen.
- Only provide your user name and password when your browser indicates an encrypted connection. An encrypted connection is normally indicated by an "https://" in your browser's address bar in front of the address of the page you are visiting. Although every browser is different, generally an encrypted connection is denoted by an image of a closed lock in the lower right-hand side of the browser window.

Protect your identity

How to protect yourself from identity theft

Identity theft is one of the fastest growing crimes in America. Taking a few easy precautions can help you protect yourself against identity theft.

Because you can control the information you choose to release, you are the single best person to protect your personal information. Some easy ways to do this include keeping anything that contains personal or account information in a safe place, providing your information only to trusted sources and reducing the amount of mail you receive with your personal information on it.

You can help minimize your risk of becoming a victim of identity theft by following these tips:

- Never provide your personal information to unknown telephone callers or e-mail solicitations. This information includes checking account information, credit card numbers, Social Security number, etc.
- Never give anyone your ATM, check card or credit card PIN. Retailers and banks (including the bank that issued your card) should never need your PIN for verification.
- Always review your bank statements and report discrepancies or suspicious transactions immediately.

- Report lost or stolen credit cards, check cards, ATM cards or checks as soon as you realize they are missing.
  - Put checks and bank documents (including statements, cancelled checks and credit/debit card receipts) in a secure location so they are not accessible to guests, contractors, repairmen, etc.
  - Destroy documents that contain your personal information before you discard them (credit card offers you get in the mail, financial statements, cancelled checks, etc.).
  - When entering credit/debit card information into an online shopping page, be sure the web page is secure and the retailer is a reputable company. The address bar on your Internet browser will show if a web page is secure. A secure web page will start with "https://" and is generally denoted by an image of a closed lock in the lower right-hand side of the browser window. A page that is not secure starts with "http://" and does not have a lock in the lower right corner.
  - Do not share login access information for online banking, online brokerage or other online accounts with third parties.
  - Do not carry your Social Security card in your wallet/purse.
  - Regularly check your credit report from each of the credit bureaus—report discrepancies to them immediately. You are entitled to one free credit report annually from the three major credit bureaus. Visit www.annualcreditreport.com for more information.

What to do if you become a victim

If you become a victim of identity theft, immediate action is required. Take the following actions to protect your personal and financial interests:

Step 1: If you suspect you might be a victim of identity theft, contact the three major credit bureaus listed below to place a fraud alert on your credit file and report identity theft.

Equifax
PO Box 105069
Atlanta, GA 30349
To order a credit report: 800-685-1111
To report credit fraud: 800-525-6285
http://www.equifax.com

Experian
To order a credit report: 888-397-3742
To report credit fraud: 888-397-3742
http://www.experian.com

Trans Union
PO Box 1000
Chester, PA 19022
To order a credit report: 800-916-8800
To report credit fraud: 800-680-7289
http://www.transunion.com

Types of alerts

Initial alert

- Stays on your credit report for at least 90 days.
- Request the alert when you suspect you are a victim of identity theft (stolen wallet/purse, lost credit card, victim of "phishing scam").
- You are entitled to one free credit report from each of the bureaus.

Extended alert

- Stays on your credit report for a period of seven years.
- Only authorize if you have been an identity theft victim.
- Only authorize after an identity theft report is filed.
- You are entitled to two free credit reports during the first year after the fraud alert is added.
- Remove yourself from marketing lists for pre-screened credit offers.

Please contact the Direct Marketing Association at 212-790-1500, ext. 1888, to be removed from the marketing lists. Or go to www.dmaconsumer.org for more information.

If you do not wish to receive pre-approved offers of credit or insurance in the mail, you can have your name and address removed from pre-screened mailing lists obtained from credit bureaus by calling: 888-5OPTOUT (888-567-8688) or going to www.optoutprescreen.com.

Important: Keep a record of all your communications. Keep copies of all letters. Send letters by certified mail.

Mail fraud: if someone stole your mail/changed your address, immediately contact the post office and file a complaint. Contact your state's Department of Motor Vehicles if you suspect someone stole your driver's license number.

Step 2: Close the accounts that you know have been opened fraudulently. Contact each company's fraud department and request a fraud affidavit to dispute the account and/or transaction.

Step 3: File a report with your local police department or with the police department in the community where the identity theft took place.

Step 4: File a complaint with the Federal Trade Commission at http://www.consumer.gov/idtheft or call 877-IDTHEFT (877-438-4338; TTY 866-653-4261) or write: Identify Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Step 5: Continue to monitor your credit reports. Correct all mistakes by writing to the reporting agencies. Send the letter "return receipt" requested.

UBS Financial Services Inc.
ubs.com/fs
2018-37638

UBS