



Protect Yourself from Fraud



© 2016 Wells Fargo Bank, N.A. All rights reserved. Member FDIC.

Goals for today

1. Raise awareness of exactly how your personal information can be stolen
2. Learn how identity thieves operate
3. Develop a plan to protect yourself from the theft of your identity
4. Learn how to report fraud, identity theft and suspicious activity when it occurs



Identity theft vs. identity fraud

<p>Identity theft Identity thieves use stolen personal information, such as a Social Security number or bank account number, to open accounts or initiate transactions in your name. Identity theft may cause financial loss or damaged credit.</p>	<p>Identity fraud Identity fraud is usually limited to an isolated attempt to steal money from an existing account, such as a charge on a stolen credit card.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

How identity thieves get your personal information

- Dumpster diving
- Skimming
- Phishing
- Hacking
- Old-fashioned stealing



Source: Federal Trade Commission (FTC)

3

Recognizing how identity thieves operate

To protect your identity, it's vital to understand more about how fraudsters operate. Typical methods include:

- Fraudulent emails, websites and phishing
- Other scams, such as fraudulent phone calls and job scams

4

Fraudulent emails or phishing

What is phishing?

Phishing involves soliciting information under false pretenses via email or a website. Phishers pretend to be a company or financial institution and send email messages to get you to reveal your personal information.

What should I look for?

Many phishing emails will express an "urgent" need for you to take action to:

- Update your information
- Activate your online banking account
- Verify your identity by clicking on a link

5

Learn to recognize fraudulent emails

Typical signs of phishing:

- Awkward greeting
- Typos
- Incorrect grammar
- Strange or unfamiliar links when you place your mouse cursor over a link
- Compelling or urgent language
- Company or financial institution name spelled incorrectly



How fraudsters obtain email addresses

- On the Internet
- By purchasing email lists
- By taking an educated guess



Fraudulent websites – phish or spoof websites

- How do I know if a website is phony?
- Consider how you got to the site
- Use caution if you followed a link in a:
 - Suspicious email
 - Suspicious text message
 - Suspicious online chat
 - Pop-up window that requests your personal or account information

Other scams

- Job scams
- Lottery or sweepstakes scams
- Dating scams
- Internet scams
- Telephone scams
- Mortgage scams targeting both prospective and current homeowners



If it sounds too good to be true, it probably is! If you believe you are the victim of a scam involving your bank or another company, contact them immediately.

9

General fraud prevention tips

1. Carry only necessary information with you.
2. Make photocopies of vital information you carry regularly and store in a secure place.
3. Do not provide your Social Security number unless absolutely necessary.
4. Reduce the use of paper.
5. Shred papers containing personal and financial information before recycling.
6. Place outgoing mail in a U.S. Postal Service mailbox.
7. Promptly retrieve incoming mail.
8. Know your billing and statement cycles.

10

Review and monitor your credit status frequently

Request a free copy of your credit report at least once a year. Each of the three major credit agencies is required by law to provide you with a free credit report annually at www.annualcreditreport.com.

Tip:

Be sure to go to www.annualcreditreport.com for your free report. There are many look-alike sites which are not free of charge!

You can also request additional credit reports anytime by paying a small fee:

Equifax:
1-800-685-1111
www.equifax.com

Experian:
1-888-397-3742
www.experian.com

TransUnion:
1-800-916-8800
www.transunion.com

11

Online security tips

1. Use a current web browser.
www.wellsfargo.com/help/wfonline/browser_supported
2. Avoid downloading programs from unknown sources.
3. Do not use your Social Security number as a username or password.
4. Change your usernames and passwords regularly and use combinations of letters, numbers, and "special characters" such as "pound" (#) and "at" (@) signs.
5. Do not use your online banking password as a password for other online accounts.
6. Protect your personal and account information
7. Use secure websites for transactions and shopping.
8. Always log off from any website after making a purchase with your credit or debit card. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.
9. Close your browser when you're not using the internet.
10. Share your confidential information with care.

12

Email security tips

1. Be wary of suspicious emails.
2. If you receive a suspicious email that you think is a phish email, do not respond.
3. If you mistakenly respond to a phish email and give out your personal information, report the incident to the involved company or financial institution as soon as possible.



13

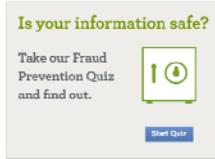
If you become a victim of identity theft

- Report fraudulent emails and websites.
- Report identity fraud and identity theft.
- Report suspicious activity.
- Utilize the Wells Fargo Identity Theft Repair Kit to organize your response to fraud.
www.wellsfargo.com/privacy-security/fraud/repair-kit



14

Fraud Prevention Quiz



Take the Quiz!

www.wellsfargo.com/privacy_security/fraud/protect/quiz

15

How will you protect your identity?

- What did you learn today?
- What will you take away from this seminar and put to use in your life?
- Questions?



16

Thank you

Thank you for participating in today's *Wells Fargo At Work* workshop.

Please complete our evaluation form to tell us what you thought of our presentation and how we can make it better.

17
