
SHARING ISN'T ALWAYS GOOD!



A PRESENTATION ON IDENTITY THEFT

MARITTA BUSH, JUMP\$TART REGIONAL DIRECTOR

**2010 IOWA JUMP\$TART
PERSONAL FINANCIAL LITERACY CONFERENCE
JULY 22 & 23**



WHAT IS IDENTITY THEFT?



IDENTITY THEFT OCCURS WHEN SOMEONE USES YOUR PERSONALLY IDENTIFYING INFORMATION (NAME, SSN, CREDIT CARD NUMBER, ETC.) WITHOUT YOUR PERMISSION, TO COMMIT FRAUD OR OTHER CRIMES.

SOURCE: THE FEDERAL TRADE COMMISSION WWW.FTC.GOV/IDTHEFT





SOME STATISTICS

**ACCORDING TO THE BOSTON FEDERAL RESERVE:
“THE FBI CALLS IDENTITY THEFT ONE OF THE
FASTEST GROWING CRIMES IN THE U.S. AND
ESTIMATES THAT 500,000 TO 700,000
AMERICANS BECOME IDENTITY THEFT VICTIMS
EACH YEAR.”**



TYPES OF IDENTITY THEFT CRIME



- Personal Information

- SSN

- Drivers License

- Credit Cards

- ATM/Debit Cards

- Checks



How Do THEY Do It?



- On-Line Theft
 - Phishing
 - Pharming
- Scamming
- Skimming
- Credit Card Readers
- Wireless Theft
- Physical Theft
- OMG! The Social Networks





PHISHING & PHARMING

Helping Consumers Avoid Internet Fraud

Federal Reserve Bank of Boston

PHISHING is a form of online identity theft that lures consumers into divulging their personal financial information to fraudulent web sites, known as *spoofed web sites*.



Great Western Bank
Making Life Great Member FDIC

Online Banking

Update your Great Western Bank Information

From: Great Western Bank onlinebanking@greatwesternbank.com

To:

Dear customer,

Security is a priority at Great Western Bank. We are committed to protecting the security and confidentiality of your personal and financial information. We use a combination of state-of-the-art technology and methods to help to protect your security.

From guaranteeing your online payments will go through, to monitoring your online and offline banking transactions for potential fraudulent activity, Great Western Bank works constantly to provide for the security and dependability of your banking.

There have been a recent increase in the number of identity theft attempts targeting Great Western Bank customers. Please note that we have no particular indication to show that your information have been compromised in any way. However, we require you to update your information as a precautionary measure against fraud.

To securely update your Great Western Bank information please go to:

<https://www.greatwesternbank.com/netteller/>

Thank you for your prompt attention to this matter and for banking with Great Western Bank!

Regards,

Matilda O'Reilly,
Head of Great Western Bank® Identity Theft Department.

Copyright © 2010 Great Western Bank.

All rights reserved.

Do not reply to this email as it is an unmonitored alias.



Your account access has been limited for the following reason(s):

Dear member,

PayPal is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Why is my account access limited?


We have reason to believe that your account was accessed by a third party. We have limited access to sensitive PayPal account features in case your account has been accessed by an unauthorized third party. We understand that having limited access can be an inconvenience, but protecting your account is our primary concern. (Your case ID for this reason is **PP-539-501-5802**.)

How can I restore my account access?

Please visit the [Resolution Center](#) and complete the "Steps to Remove Limitations."

Completing all of the checklist items will automatically restore your account access.

You can also verify your account by logging into your PayPal account at:

 <https://www.paypal.com/us/>

Thank you for using PayPal!

ase do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to PayPal account and choose the Help link located in the top right corner of any PayPal page. To receive email notification in plain text instead of HTML, update your preferences [here](#). PayPal Email ID PP468

PHARMING is similar to phishing, but is more sophisticated. Pharmers send emails which contain a virus (or Trojan horse) that installs a small software program on the user's computer when the consumer opens the email. The next time the consumer visits his/her official financial site, the program redirects to a spoofed web site which captures personal information.



PHISHING & PHARMING

Helping Consumers Avoid Internet Fraud

July, 2010

Iowa JumpStart Personal Financial Literacy
Conference

9
Federal Reserve Bank of Boston

SCAMMING



- Nigerian Letter
- Investment Scams
- Loan Scams
- Charitable Giving Scams
- Disaster Scams



SKIMMING

Relating to ATM and Debit Cards . . .

Skimming occurs when thieves set up a device that captures the magnetic stripe and keypad information from ATM machines and gas pumps.

Source: ABA Education Foundation www.aba.com/ABAEF/debitcardfraud.htm



SKIMMING, CONT.

Relating to ATM and Debit Cards . . .



SKIMMING AT THE GAS PUMP



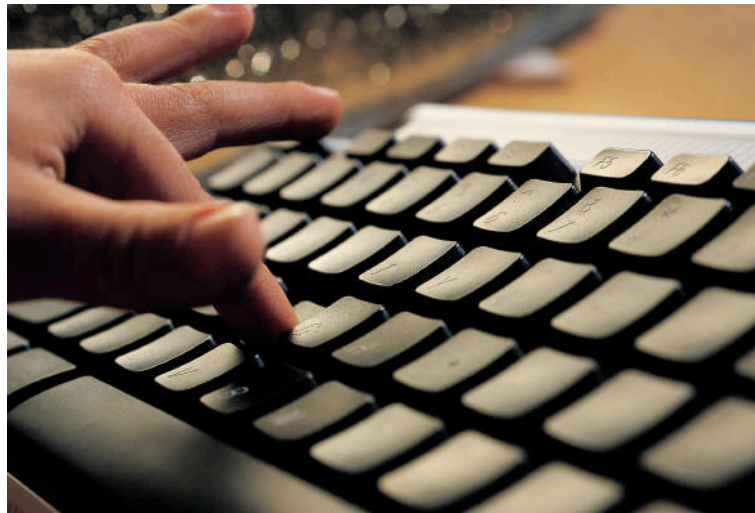
- Relates to Debit Cards
- Device is Attached Inside the Gas Pump
- Completely Invisible



CREDIT CARD ACCESS



WIRELESS ID THEFT



- 🌊 Surfing in Public Places
 - ✈ Airports
 - ☕ Coffee Shops, Restaurants
- 🏠 Surfing While You Are In Your Home



OMG ~ THE SOCIAL NETWORKS



YouTube

twitter

facebook

MySpace.com

Networks for:

- General and Friends-based
- Hobby and Special Interest
- Movie and Music
- Pets
- Business/Professional
- Reading and Books
- Mobile

hi5



SHARING ISN'T ALWAYS GOOD!

CAN ID THEFT BE PREVENTED?



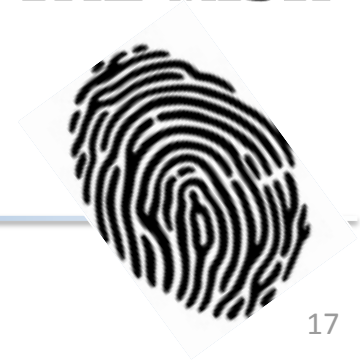
SADLY, NO.

HOWEVER . . .



1. WE **CAN** MAKE IT TOUGH FOR THIEVES TO SUCCEED.

2. WE **CAN** TAKE STEPS TO MINIMIZE THE RISK AND RESULTING DAMAGE.



PROACTIVE MEASURES



1. Physically secure your SSN (don't carry it); keep track of your driver's license, your credit cards and ATM/debit cards and their PINs.
2. Let's talk about the U.S. Postal Service.
 - a. Incoming mail
 - b. Outgoing mail



PROACTIVE MEASURES, CONT.

3. Keep your computer software with the latest virus and anti-spyware, adware, malware, firewalls etc. available. Use passwords; change them every 3-6 mos. Don't store passwords on your computer.
4. Resist the temptation of putting sensitive, personal info on social networks.
5. Frequently monitor financial accounts and billing statements, preferably online; then log-off and close your browser.
6. Pull your credit report annually – www.AnnualCreditReport.com
7. Shred sensitive documentation that contains personal information.





RESOURCES



In Iowa

Iowa Attorney General Office, Consumer Protection Division
Dept. of Transportation, Office of Motor Vehicle Enforcement

Other Resources

Federal Trade Commission (FTC), Consumer Response Center: www.ftc.gov

Booklet: *Social Networking Sites: Safety Tips for Tweens and Teens*

www.OnGuardOnline.gov

To stop a phisher, pharmer or spoofer, forward email to: spam@uce.gov

Federal Reserve Bank of Boston

Brochure: *Identity Theft* www.bos.frb.org/consumer

iKeepSafe.org - founded by 49 governors/first spouses, law enforcement & the AMA
www.iKeepSafe.org



THANK YOU



FOR LISTENING

STAY SAFE



KEEP OUR CHILDREN SAFE

FROM IDENTITY THEFT
