Pioneer Bank

PRESENTED BY:

JEFF WHITROCK
PRESIDENT AND CEO OF PIONEER BANK
1.715.652.2131

Go to our web site
http://www.pioneerbank.net/idtheft.html
to view an identity theft guide for individuals and businesses.

Top 10 Ways Personal Data is Breached

#1. Losing or having your laptops/PCs/computer storage devices stolen

#2. Phishing/pharming/vishing

#3. Employee theft of information

#4. Information bought by a fraudulent business

#5. Employees allowing access to information

#6. Poor business practices (no dual control)

#7. Internal security failures

#8. Viruses/trojan horses/security loopholes

#9. Improper disposition of information

#10. Information tossed into trash cans/dumpsters

* According to NABS (National Association for Bank Security)

New Scams

Scam #1: "Phishing"

Scenario:
With this technique computer hackers use email to "fish" the internet, hoping to "hook" you into giving your personal information to them, which the hackers do not have unless you provide it.

Commonly Poses As: internet provider, bank or school

Scam #2: New Shopping Department Store Promotion

Scenario:
You receive a message or call that you've "won" a drawing at the new store. Someone from the store will wire you the money, as long as you provide a routing and checking account number.

Scam #3: Secret Shopper "Work From Home" Scam

Scenario:
After receiving a check for $5,000, you're told to be a "secret shopper" for major stores (like McDonalds, Best Buy, Walmart, Burger King, GAP and UPS) and to purchase gift cards with your own cash. As directed, you mail the gift cards to their address to later find out that the original $5,000 check was fraudulent - usually, it's too late.

Scam #4: Credit Card Scam

Scenario:
You receive a phone call that you were in Las Vegas yesterday, which you were not. As a result, you are lead to believe that the caller thinks someone used your card. Then, he or she offers to cancel it for you but will need to verify your card number, which the caller does not have unless you provide it.

Commonly Poses As: credit card company or bank

Scam #5: Phone "Vishing"

Scenario:
The victim receives an email or phone call that his or her account has been frozen. In addition, the victim is instructed to call an 800 number to remove this "freeze" and is prompted to enter, for an example, an account number or PIN. Finally, he or she is told the account has been unlocked. In actuality, it was never frozen.

Scam #6: Phone "Phishing"

Scenario:
Victim is usually an elderly person. Initially, the fraudulent caller only has half the correct information of the victim. However, during the conversation, the victim unknowingly corrects the inaccurate information, giving up his or her personal information.

Pioneer Bank

PRESENTED BY:
JEFF WHITROCK
PRESIDENT AND
CEO OF PIONEER BANK
1.715.652.2131

New Scams

Scam #7: Mail Scam

Scenario:
You have just won the lottery! By mail, you receive a cashiers check for a couple thousand dollars to cover taxes. Next, you're informed to cash it at your bank and wire the money to the named location (usually outside the USA). After the money is wired out, you realize the original cashiers check is no good.

Scam #8: Postal Money Order Scam

Scenario:
Very easy to duplicate - a fraudulent postal money order is sent to a victim to cash. However, this scam can be prevented by calling the post office to verify the postal money order number.

Scam #9: eBay Scam (Selling Products Online)

Scenario:
The victim receives a message from someone offering to pay more than the asking price for an item if you cash the check and send back the extra money. However, the original check is fraudulent. * If it seems too good to be true, it probably is.

Scam #10: Nationwide Security Office Scam

Scenario:
The victim is told his accounts were compromised and must provide personal information to the caller to prevent more fraud as soon as possible.

Scam #11: Deceased Scam

Scenario:
Identity thieves can obtain a name, address and birthdate from an obituary. Then, they purchase the decedent's social security number and credit history.

To Help Reduce the Risk:

1. All credit cards and charge cards should be cancelled as soon as possible after death.
2. Cancel the driver's license at DMV (Department of Motor Vehicles) and refuse requests for duplicates as soon as license is taken away.
3. Send a copy of the death certificate to credit bureaus.
4. Once a personal representative is authorized to act on the behalf of the deceased, obtain the free credit bureau reports to be sure there has been no post-death activity.

Scam #12: IRS Scams : Sizeable Rebates for Filing Taxes Early

Scenario:
The fraudulent caller asks for more personal information for the rebate and if the victim refuses, the caller threatens to withhold the rebate.

IRS Audit Scam

Scenario:
The customer is told his or her tax return will be audited and is asked to use "links" provided to fill out the information to start the process.

IRS Law Email Scam

Scenario:
This fraudulent email advises you to upload new updates, when actually you've been tricked into downloading malware on your computer, which gives remote access, password access, etc. . . to outlaws.

Common Targets: businesses, accountants or money managers

Fact: All IRS web pages begin with http://www.irs.gov/. The IRS does not send out unsolicited emails or ask for detailed personal information via email. Additionally, the IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.

Proactive Solutions:

1. Use email alerts to increase awareness of activity.
2. Reduce paper statements with e-statements.
3. Stay alert to phishing scams. Know your 2 step online authentication process (88% banks/48% phones).
4. Frequently review bank accounts and credit bureaus. Get 1 free credit bureau each year at www.annualcreditreport.com.
5. Don't use or give out your full social security number.