

# SECURING YOUR ACCOUNTS

## Financial Position

Investing

Estate Planning

Managing Risk

Retirement Planning

Taxes

*How do you protect your credit and identity in this age of frequent credit and identity theft? Take measures to prevent the nightmare before it occurs. Please consider these key suggestions you may not find elsewhere for securing your credit.*

## Use Unique E-mail Addresses

Many people use only one e-mail address. This is potentially dangerous as an Internet security breach at a company you do business with can expose your e-mail address and other information to hackers. These types of breaches are common. If you use a unique e-mail address just for your financial institutions, it will be harder for thieves or acquaintances to guess it.

And consider using different e-mail addresses for friends, family, and merchants. This will isolate you from problems that may arise and helps protect your financial accounts. Free e-mail addresses are available from Google, Microsoft, Yahoo, and others.

<http://mail.google.com>

<http://www.hotmail.com>

<http://mail.yahoo.com>



## Use Unique Passwords

If you use the same password for every company you do business with, you put all your accounts in jeopardy if that password is exposed. Use a different, complex password for every company you do business with.

The best passwords are at least ten characters; use both upper and lower case characters, numbers, and symbols. For greater security, use longer passwords up to 25 characters. Avoid using names and words in the dictionary, and names, dates and other terms that are personally significant to you. If you need help remembering a password, try an acronym by taking the first letter of each word in a sentence and substituting numbers or symbols where appropriate. Change your passwords periodically, at least once every year or two.

Additionally, when asked for your mother's maiden name, in most cases businesses only know what you tell them. Provide a different unique name that only you know.

## Get Your Bills Electronically

Receive all your bills and statements electronically and stop receiving paper statements. This avoids lost or stolen mail. And it gives you access to PDF copies of your statements for long-term reference. If electronic delivery isn't available, consider a PO Box for receiving such mail.

## Copy Your Credit Cards

Copy both sides of your credit cards to capture account and contact numbers. If you lose a card, having that data makes it easier to cancel a stolen card.

## Prevent Check Washing

Check washing is done by thieves who wash away the ink from your check, while protecting your signature, so they can change the name and amount. The easiest way to prevent check washing is to reduce your use of checks. But if you need to pay with a check instead of cash, money order, or credit card, then use a special pen to help protect you. Uni-ball 207 gel pens, shown at [www.uniball-na.com](http://www.uniball-na.com), use specially formulated inks that become trapped in paper.

## Reduce Preprinted Check Information

Don't have your full name printed on checks as thieves will know what name to sign. Instead, use just your initials. Consider leaving off your address, phone number, and Social Security number, which aren't required. This reduces data available to identity thieves and people who may target your home.

Even with reduced preprinted information, your account number still appears on checks. If someone steals your checks, the thief may reorder checks and have them sent elsewhere. Don't have new checks mailed to your home where they can be stolen from your mailbox – tell the

bank you want to pick up your checks. Remember, to be safer, reduce your use of checks and use safer payment methods such as money orders.

## Use a Shredder

Many thieves enjoy going through your trash and finding sensitive documents you have thrown away. Shred pre-approved credit offers, as thieves can order credit cards in your name and mail them to their address. Also shred courtesy checks, receipts, bills, anything with your name and address, and other sensitive information.

Different types of shredders are available. Avoid strip-cut shredders that produce long strips of easily reassembled paper and get a cross-cut or confetti-cut shredder that reduces paper to tiny squares.

## Protect Your Social Security Number

While Social Security numbers are widely used for identification for which they were never intended, their required use is diminishing as companies substitute alternate numbers. Many individuals and forms may ask for your Social Security number, but often it isn't needed or required. Be sure who you are giving any personal information to and if it is truly needed.

## Get a Passport for Identification

Even if you think you'll never leave the country, get a passport or the new, wallet-size passport card for identification from <http://travel.state.gov/passport>. It has your name and birth date, but doesn't have your home address like your driver's license does.

A passport is great for identification even outside of an airport, especially since driver's licenses are more easily duplicated, are a common key to stealing your identity, and most states sell data from driver's licenses. And it is possible that passports will be required to fly domestically in the future.

Use your passport for identification when you cash a check. If a teller writes your passport number on the check, thereby giving your number to the check owner, at least they won't have your driver's license number, which can potentially expose you to identity theft.

## Simplify Your Wallet

Don't carry your Social Security card, extra credit cards, or sensitive documents in your wallet or purse except when necessary. This practice minimizes the amount of information a thief can steal.

## Be Wary of Social Engineers

In an effort to gain access to your accounts and life, thieves may call or e-mail pretending to be from your bank, merchant, or other company. They may say that your account has been compromised and that you need to give them passwords and other sensitive personal and financial data to reinstate your account.

If they have successfully stolen some of your information, they may convey those facts to make them sound more real and in authority. Mailing addresses, account numbers, transactions, and birthdays are easily obtained, and most of that information is on statements that can be stolen from your mailbox. Don't fall for this scam that enables the perpetrators to commit identity theft and credit card and bank fraud.

If you receive an unsolicited call from a financial institution, don't give out your information. Financial institutions should not ask for your information, except to verify your identity when you call them. And be aware that Caller ID can be faked.

Never reveal personal or financial information in a response to an e-mail request, no matter who appears to have sent it. E-mail addresses can be easily faked, or the sender's computer may be infected with a virus that is sending e-mail without the sender's knowledge. PayPal, eBay, and banks are common targets.

When unsure of such communication, call the company or visit the company Web site. Don't click on links in e-mail that can take you to a fake Web site that looks identical to the real site. Instead, type the Web address into your browser. Make sure you spell the Web address correctly, as fake Web sites use common and subtle misspellings of real sites.

Security consultant Kevin Mitnick has written excellent books on social engineering. If you want to be more aware of fraudulent practices, visit <http://mitnicksecurity.com/products.php>.

FINANCIAL PLANNING *at* DESERET MUTUAL BENEFIT ADMINISTRATORS

60 East South Temple • Salt Lake City, Utah 84111  
Telephone 1-801-578-5627 • Toll Free 1-800-777-3622, ext. 5627 • Fax 1-801-578-5933  
[finplanning@dmba.com](mailto:finplanning@dmba.com) • [www.dmba.com](http://www.dmba.com)