

# Information Privacy & Security Month

## Week 2: Personal Financial Records

### Financial Records

Even before the advent of e-commerce, personal financial information was something easily stolen or misappropriated. Thieves would cull trash receptacles looking for old checks, billing statements from credit cards or other financial transactions. Thieves still practice the fine art of dumpster diving in the hopes of retrieving such valuable information, but now they also prowl the internet. It is more important than ever to be aware of what kinds of financial information exist, the kinds of threats posed by unauthorized use of such information, and what can be done to protect oneself against fraudulent use of financial assets and identity theft.

### Sensitive Information

The first step in protecting your personal financial records is to be aware of what kinds of information can be used to gain unauthorized access to your finances. Obvious concerns include social security numbers, bank account numbers, checks, credit card account numbers, credit and debit cards themselves, bills from creditors, receipts from credit transactions, and official documents (driver's license, passport, birth certificates, etc). It is essential to safeguard such sensitive information, and to take appropriate action immediately if it is ever lost or stolen.

### When Sensitive Information is Compromised

- **Social Security Number** Your SSN is the mother lode when it comes to sensitive information. Once compromised, social security numbers can be used to gain access to all kinds of financial, health, and other personal information. If your social security number is lost or stolen you should immediately call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. This alert can help stop someone from opening new credit accounts in your name.
  - **Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241
  - **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 2002, Allen, TX 75013
  - **TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- **Bank Account Numbers, Checks, and Debit Cards** Consult with your financial institution about whether to close bank or brokerage accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts that you open. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.
- **Credit Cards** Contact the credit card company immediately to inform them of the compromise. Ask them to close the account immediately and provide a novel password on any new accounts opened. You can also ask that they monitor the account for fraud.
- **Official Documents (Driver's License, Passport, etc)** Contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include:

- receiving credit cards that you didn't apply for;
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter. For more information on getting your credit reports free once a year or buying additional reports, read *Your Access to Free Credit Reports* at [www.ftc.gov/bcp/online/pubs/credit/freereports.htm](http://www.ftc.gov/bcp/online/pubs/credit/freereports.htm).



# Information Privacy & Security Month

If your information has been misused, file a report about your identity theft with the police, and file a complaint with the Federal Trade Commission at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Read *Take Charge: Fighting Back Against Identity Theft* for detailed information on other steps to take in the wake of identity theft.

## Prevention

All the procedures mentioned so far provide tactics for remediation once sensitive information has been compromised. By far the best approach to protecting your sensitive financial and personal information is to prevent its being compromised in the first place. Preventing unauthorized access to paper-based transactions and information requires vigilance in disposing of sensitive information. It is important to shred any documents containing sensitive information. The documents should be finely shredded so that it is not possible to reconstitute the original document from the shredded remains.

Electronic information is another matter entirely. With the advent of e-commerce, e-mail, and sophisticated phishing scams, it is more important than ever to be aware of how to prevent illegitimate electronic access to personal or financial information.

Phishing is the act of tricking people into providing sensitive information over the internet. Phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an email or pop-up message that asks for personal or financial information, do not reply. And don’t click on the link in the message, either.** Legitimate companies don’t ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself. In any case, don’t cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.
- **Use anti-virus software and a firewall, and keep them up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It’s especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software “patches” to close holes in the system that hackers or phishers could exploit.

- **Don’t email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s website, look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL for a website that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer’s security.



# Information Privacy & Security Month

## For more information, check out the following resources

- KU Privacy Office <http://www.privacy.ku.edu> 864-9528
- KU IT Security Office <http://www.security.ku.edu> 864-9003
- KU Office of Student Success <http://www.vpss.ku.edu> 864.4381
- KU Public Safety Office <http://www.ku.edu/~kucops/> 864-5900
  
- Some relevant policies can be located in the IT Policy Library at <http://www.policy.ku.edu/it/index.shtml>.

***NEXT WEEK: What is HIPAA and why do we always have to read and sign notices at the doctor's office and pharmacy?***