

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS CONSUMER CONFIDENCE TOOLKIT: DATA SECURITY AND FINANCIAL SERVICES

SEPTEMBER 2005

A PUBLICATION
OF
BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

BITS CONSUMER CONFIDENCE TOOLKIT: DATA SECURITY AND FINANCIAL SERVICES

TABLE OF CONTENTS

INTRODUCTION

WHY CARE?

Crisis in Consumer Confidence

ROLE OF THE FINANCIAL SERVICES INDUSTRY

Financial Institutions' Leadership Role

Financial Institutions Are Highly Regulated and Supervised

CURRENT SECURITY ENVIRONMENT

Cybersecurity Threats and Vulnerabilities

Phishing, Pharming, Spyware and DNS Poisoning

Data Breaches and Notification

No Simple Solutions

Encryption

Authentication

Need for Uniform National Standards

RECOMMENDATIONS FOR GOVERNMENT AND POLICY MAKERS

WHAT CONSUMERS SHOULD KNOW AND WHAT THEY CAN DO TO PROTECT THEMSELVES

Things to Know

General Security

Online Security

FACTS AND MYTHS

Javelin Strategy and Research Results

RESOURCES

INTRODUCTION

This Consumer Confidence Toolkit provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided.

This document was developed by BITS. BITS is a non-profit industry consortium whose members are 100 of the largest financial institutions in the United States. BITS shares membership with The Financial Services Roundtable. BITS and Roundtable member companies provide fuel for America's economic engine, accounting directly for \$40.7 trillion in managed assets, \$960 billion in revenue, and 2.3 million jobs.

The CEOs of The Financial Services Roundtable established BITS in 1997. BITS is the strategic business and technology division for The Financial Services Roundtable and works on key issues where industry cooperation serves the public good, such as critical infrastructure protection and the safety of financial services. Major purposes are to develop and disseminate industry best practices for improving information security programs, reducing fraud, managing third party providers, managing risk and fostering innovation. BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

WHY CARE?

Crisis in Consumer Confidence

- There is a potential crisis in consumer confidence in the safety of the Internet for conducting financial transactions.
- Increases in phishing incidents and other forms of e-scams and online fraud are heightening consumer concerns.
- Lost and stolen data, including personally identifying consumer information, are adding to consumer fears and concerns.
- Inaccurate information could lead to poor policy decisions, including attempts at solutions that create new burdens on industry and consumers without solving problems.
- There is a need for fact-based solutions to issues concerning data security and financial services.

ROLE OF FINANCIAL SERVICES INDUSTRY

Financial Institutions Are Leaders in Addressing Cyber Security Issues and in Protecting Customers

- The financial services industry is working diligently to implement controls to combat fraud and other forms of cyber crime.
- Financial institutions use a variety of safeguards to ensure the reliability and security of financial transactions, and protection of financial privacy. Many of these safeguards are required of financial institutions by federal regulators.
- Financial institutions use systems to monitor customers' account activity and analyze patterns to detect and prevent unusual or fraudulent activities.
- Experts from financial institutions develop and share best practices and other voluntary guidelines to safeguard information and manage cyber security risks.
- Financial institutions know that identity theft is a serious concern of consumers and are working proactively to prevent the crime as well as to assist those who fall victim to it.
- Many institutions provide a 100% online guarantee in the event of online fraud.
- Financial institutions are educating customers on steps they can take to secure their computers and to avoid the lure of fraudsters to supply confidential information or access information such as passwords or PINS.

Examples of Financial Services Sector's Leadership Role

1. Assisting Victims of ID Theft

- **BITS and The Financial Services Roundtable established the Identity Theft Assistance Center (ITAC) in 2004.**
 - ITAC provides a free victim assistance service for customers of member companies. ITAC helps victims of ID theft by reducing the delay and frustration that consumers often experience as they restore their financial identity.
 - As of August 2005, the ITAC has helped more than 2000 consumers restore their financial identities.
 - The ITAC information is shared with law enforcement to help prosecute the perpetrators.
 - The ITAC is a cornerstone of our overall industry efforts to detect and prevent fraud, help victims, address the causes of identity theft and enable prosecution of fraudsters.

2. Urging Software Vendors to produce more secure software products

- BITS issued Software Security Business Requirements to encourage software companies to reduce vulnerabilities in their products and to make the “patching” process more efficient and effective. Vendors have been responsive. One major provider has implemented a work plan to meet BITS’ requirements.

3. Sharing Information on threats, vulnerabilities and incidences

- BITS/FSR helped to establish and continues to support the Financial Services Information Sharing and Analysis Center (FS/ISAC).

4. Gathering Intelligence to Detect and Respond to Fraudsters

- BITS created the BITS Phishing Prevention and Investigation Network to help shut down online scams, aid in investigating perpetrators by providing data to law enforcement, and providing a “united front” for combating online schemes.

Financial Institutions Are Highly Regulated and Supervised

- The financial services industry is both highly regulated and supervised by federal regulators (Federal Deposit Insurance Corporation, Federal Reserve System, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Security and Exchange Commission) and state regulatory agencies.
- Examiners from regulatory agencies routinely audit financial institutions and service providers and support the financial services industry. As part of these examinations, experts in information security assess the adequacy of controls that financial institutions have in place. When deficiencies are detected, the regulators mandate changes or impose sanctions on financial institutions.
- Federal and state examiners constantly evaluate the controls financial institutions have in place to protect the privacy and security of customers.
- When there is a security breach that could result in potential harm to a customer, the federal regulators require that financial institutions promptly contact those individuals.

CURRENT SECURITY ENVIRONMENT

Cybersecurity Threats and Vulnerabilities

- Cybersecurity threats are increasing.
- Criminals are writing code to compromise systems.
- Software viruses are a significant challenge facing the software industry.
- Hackers are closing the window between the discovery of a flaw and the release of a new virus.
- Software vulnerabilities and exploits are too high and increasing.
 - Over 1200 new security flaws were discovered during the last six months of 2004.
 - In early 2004, BITS surveyed its members to estimate the costs to financial institutions of addressing software security and patch-management problems. Based on the survey, we estimate that it costs the financial services industry nearly \$1 Billion annually to deal with software security and patch management problems.
- Criminals have better tools for breaking into computer systems and networks. Law enforcement must do more to deter against crime by prosecuting cyber criminals and working with foreign law enforcement agencies and international organizations.

Phishing, Pharming, Spyware and DNS Poisoning

- New kinds of fraud such as phishing, pharming, spyware and Domain Name Server (DNS) Poisoning are a challenge.
 - **Phishing:** a fraudster sends an e-mail to consumers, falsely claiming to be from a legitimate company, in hopes of luring consumers to a “spoofed” website. The spoofed website mimics the legitimate website for the sole purpose of stealing the consumer’s personal information. At the typical spoofed website, consumers are asked to update sensitive personal information, such as names, account and credit card numbers, passwords, Social Security numbers and other information. Phishing targets are not limited to financial institutions, as Internet service providers, online retailers and the federal government have all been targeted. These entities often do not have the level of data security in place that financial institutions do, and are not subject to the same regulatory scrutiny as financial institutions.
 - **Pharming:** a form of malicious redirect for Internet users. It occurs when an Internet user is redirected to a criminal's spoofed site even though the user entered a valid URL in the browser's address bar. This redirection usually involves worms and Trojans that attack the browser address bar and exploit vulnerabilities in operating systems and the Domain Name Servers (DNS) of compromised computers).
 - **Spyware:** any software that covertly gathers user information through the user's Internet connection without his or her knowledge.
 - **DNS Poisoning:** the corruption of an Internet server's DNS system table by replacing an Internet address with that of another, rogue address. A user seeking the page with that address is redirected by the rogue entry in the table to a different address where worms, spyware, or other malware can be downloaded to the user's computer.
- A weak link in the system can create problems for many organizations. For example, the lack of security standards and requirements at unregulated Internet service providers and hosting companies may be facilitating the growth of phishing by providing an on-going source of easily accessible sites for criminals to use to perpetrate these scams.

Data Breaches and Notifications

- We are hearing more and more about security breaches and data losses. Data breach disclosures reflect the fact that organizations are required to report security breaches.
 - These are mandated by state laws and for financial institutions these are mandated by regulations linking back to the Gramm-Leach-Bliley Act.
- Most of these breaches are physical breaches or lost data as it was being shipped from one facility to another. There also have been hacking-related breaches and insider abuse.
- While news of these breaches sounds alarming, there is not a one-to-one correlation between the exposure of personal information in a breach and an incident of identity theft. The vast majority of compromised data never gets used.
- Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence in the financial services industry and the economy overall.
- Care must be exercised in alerting consumers to steps they can take to protect themselves from ID theft and other forms of fraud while averting needless alarm.

No Simple Solutions

- Media reporting of cyber security issues often overstates the problems and implies simple solutions. The impact of media reports is a factor in undermining consumer confidence in the financial services industry.
- Consumer fear about online security is the number one reason that consumers give for not conducting financial transactions online. Yet, monitoring financial accounts online and using electronics rather than paper can actually reduce consumers' risk of identity theft.
- Protecting privacy and maintaining security is an ongoing process. It requires constant vigilance. There are no simple solutions.
- A robust information security program has three major components: people, processes and technology.

Encryption

- Data breaches are drawing greater attention to the role of encryption.
- Encryption is an important and useful tool. In general, financial institutions regard encryption as important, useful, and a key component of their information security programs.
- Encryption is not a simple solution and the issues are complex and multi-faceted. Furthermore, encryption is a control. Its application must be measured against the need to access data today as well as to meet recovery and retention requirements in the future.
- Encryption of data poses a number of significant challenges that must be considered.
- Encryption does not protect data that is on paper, film or microfiche. Given that many of the publicly announced data breaches during the past eight months were from stolen paper documents or data sold to fraudulent businesses, its important to recognize that encryption would not have prevented the information from being viewed or compromised.
- Whether to use encryption depends on many factors, including how the data is stored, where it is transported, its intended usage, whether the data contains sensitive or confidential information, back-up or restoration requirements, retention requirements, etc. A major challenge is managing the encryption "keys" to the encrypted information. These challenges mount with increasing age of the information.
- There are consequences to encrypting data that must be weighed against the benefits. For example, there are potential negative effects on computer networks, the ability to detect intrusions, the reduced speed of computing, and the ability to retrieve data for back-up restoration or business continuity requirements.
- Some government agencies or third parties require that data be provided in unencrypted formats. Further, even when information is shipped securely by the financial institution, it may not always be shipped securely on return.

- Despite best efforts by financial institutions to protect information, exchanges with customers and third parties oftentimes are outside of the financial institution's control.
- Encryption in itself cannot guarantee data security. It can be part of a broader, robust information security program, and it needs to be well-implemented. Decisions on what data to encrypt and at what points to encrypt data are based on risk of disclosure and the costs and risks of encryption, as well as the need to access data to serve customers.

Authentication

- Some IT vendors and some regulators argue that current authentication procedures for online retail financial services – relying most often on a user identification name and an associated password – are no longer adequate to secure customers’ accounts against “phishing” attempts or to adequately combat ID theft.
- Two-factor authentication has many advantages and is used by many financial institutions for some high value transactions. However, two-factor authentication methods for Internet Commerce will not automatically prevent “phishing” or account takeover.
- Two-factor authentication might limit a criminal’s ability to immediately capitalize on the personal information he or she has stolen. However, criminals could still induce an unsuspecting consumer to give up important financial information through “phishing” or some other scheme, and make use of that information in some other way.
- Two-factor authentication methods involve serious practical problems and complexities. Many technologies that vendors are marketing are not at the state of maturity and could not, as a practical matter, be relied upon as a solution at this time. Others – such as the use of authentication tokens are mature today but are not practical or appropriate for many applications. For example, given the reality that customers interact with multiple financial institutions, either some means of centralizing token management and authentication needs to be devised – not something that exists today – or customers would be left with the responsibility of managing numerous tokens for their different financial accounts.
- Consumer acceptance challenges are a major impediment. U.S. consumers of financial services have not accepted solutions that involve lengthy enrollment processes or complicated processes for using the technology. Implementing such schemes would involve an extensive process of consumer education and training to familiarize consumers with these new procedures. A federal mandate to implement two-factor authentication would significantly impede consumers’ migration to the use of online financial services and could potentially impact current use of online financial services.

- Calls for simple solutions such as mandating encryptions for storing or transmitting all forms of data or mandating dual or multi-factor authentication for electronic commerce should be analyzed carefully to ensure that they are not overly complicated or complex.

Need for Uniform National Standards

- Efforts by various states and regulatory agencies raise significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of which state the consumer may live in. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multi-state presence.
 - A national standard should be risk-based and provide financial institutions with some flexibility in determining when and how to notify customers.
 - Financial institutions should notify customers when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people.
 - Companies that discover breaches in security should be allowed first to notify law enforcement authorities, as well as consumer reporting agencies, so that law enforcement authority can get a jump on any existing criminality and Credit Reporting Agencies may be better prepared for the potential volume of consumer inquiries about the impact of any breach on consumer credit history.

RECOMMENDATIONS FOR GOVERNMENT AND POLICY MAKERS

BITS is sought to provide expert testimony, including at Congressional Hearings, on issues related to critical infrastructure protection, cyber security, and other topics at the intersection between technology, commerce and financial services in the US economy. BITS provides input to the Federal Government's efforts to strengthen cyber security and consistently urges the Government to implement provisions outlined in the "National Strategy to Secure Cyberspace." BITS also participates in an ongoing dialogue on cyber security issues among financial institutions, leading software providers, Internet service providers, and government officials, including law enforcement and regulatory agencies. BITS has developed the following recommendations.

What Government and Policy Makers Can Do to Strengthen Cybersecurity: PREPARE©

The following are seven elements of steps the Government can take to strengthen cybersecurity. Any easy way to remember this is by the acronym, PREPARE.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.

- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.
- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

- Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.
- Train government employees on proper cyber security measures.
- Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and

educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

WHAT CONSUMERS SHOULD KNOW AND CAN DO TO PROTECT THEMSELVES

What Consumers Should Know

- Hundreds of millions of financial transactions—both online and offline—occur each day.
- On the whole, Internet banking and other online financial transactions are safer than paper-based transactions.
- Identity thefts that occur online are generally smaller and take less time to resolve than paper-based thefts.
- Identity theft is a highly complex issue with many players and no simple solutions.
- Incidents of identity theft and identity fraud are often mis-characterized in the popular media.
- Fraudulent credit and debit card transactions are not identity theft and seldom lead to identity theft.
- Most cases of identity theft do not occur online. Where the method is known, most theft of personal information is through traditional rather than electronic channels—68.2% obtained offline versus 11.6% obtained online. (Source: 2005 Identity Fraud Survey Report by Javelin Strategy and Research)
- Resolving identity theft requires coordination among multiple federal, state and local agencies, and industry.
- Consumers are protected against financial losses from fraud by laws and regulations.
- Customers will be held harmless in almost all circumstances in which fraud occurs.

- Financial institutions use sophisticated systems to flag unusual activity and protect consumers against fraud. These systems allow financial institutions to monitor activities in real time.
- Many of these controls are kept “invisible” for security reasons.

What You Can Do to Protect Yourself: General Security Tips

- **Know your merchant.** Ensure you know the person or entity to which you are giving information over the Internet, phone, or fax. Do not provide your personal information unless you have initiated contact with the merchant. Only do business with Internet companies that use a secure form, often indicated by a padlock in the lower corner of the website, to capture private information such as account numbers or credit card numbers.
- **Order copies of your credit report at least once a year** from each of the three major credit bureaus and ensure all of the information is accurate. Stagger the process so you can check your records three times each year.
Equifax 1-800-685-1111
Experian 1-888-EXPERIAN (397-3742)
Transunion 1-800-916-8800
- **Monitor your accounts and statements frequently and thoroughly,** ensuring that all activity is accurate. If your account statements are late, immediately contact your financial institution(s) to ascertain if and when the statements were mailed. If your institution offers online banking, check your account frequently and regularly, rather than waiting for monthly statements. Reporting fraud as soon as possible helps stop further occurrences of fraud.
- **Always thoroughly tear or shred documents with personal information,** such as pre-approved credit offers, which may contain account information, Social Security numbers, date of birth, etc. Shredding such documents protects you against “dumpster diving.”
- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your Social Security number and/or credit card number on a check.
- **When using your ATM, cover your hand when entering the PIN number** to protect the information from “shoulder surfers.”
- **Carry only those pieces of identification you absolutely need,** and keep them secure.

- **Check merchant privacy policies** and only shop at those that publish privacy policies with which you agree.
- **Discard unused instant credit offers**, ensuring they are properly shredded.
- **Safeguard your receipts, account numbers and account expiration dates.** Don't leave credit card records, including your transaction receipts, or anything else with credit card numbers and expiration dates in unsafe locations.
- **If you suspect your identity has been stolen or you have shared any personal financial data, including your account username and password, contact your financial institution and the authorities immediately.** U.S. consumers should:
 - File a police report with their local police department and call the Federal Trade Commission at 1-877-ID-Theft.
 - Complaints can also be reported to: the Internet Fraud Complaint Center (IFCC), www.ifccfbi.gov.
 - Contact the three credit reporting agencies to place a fraud alert on your record.
 - Maintain a log of all contacts you make with the authorities regarding the matter, including the name, title, phone number and police case number, in case future contact is required.

What You Can Do to Protect Yourself: Online Security Tips

- **Ensure your computer(s) are equipped with a security toolkit** to help keep trespassers out. A security toolkit includes personal firewalls, antivirus and virus detection software, anti-spyware software, and adware and spywareblocking software. Viruses and spyware are different, so you need to protect yourself against both. Update the toolkit frequently, and periodically check your firewall settings. Install security patches issued by your software (operating system and browser) vendor. Update software applications as well as operating systems and browsers, and be sure to patch the entire suite of applications that have the same type of vulnerability operating system.
- **Consider installing a Web browser toolbar to help protect you from known phishing websites.** A number of Internet service providers (ISPs) offer toolbars to help identify fraudulent sites. Please contact your ISP to determine which is best for you.
- **Always back up your data.**
- **Change your passwords periodically, using strong passwords that could not be easily guessed. Do not use names (like your mother's maiden name) or dates (like your birthday) or your Social Security number (SSN).**
- **Always log off from your online banking session.**
- **Shut off/disconnect your computer from the Internet when not in use.**
- **Avoid purchasing products from online merchant or auction sites if the deal looks "too good to be true."** If it looks too good to be true, it probably is.
- **Be cautious and skeptical.** If you get an unsolicited email from your financial institution asking for personal information, including your account number, contact the institution to verify its validity. Most financial institutions will NOT request such information from you via email or phone.

- **Don't click the link.** If you are concerned about the authenticity of an email, contact your financial institution directly by phone. You may also go directly to your institution's site by typing the URL in the browser. Should you choose to go directly to the site, check for indicators that the pages are secure. A secure site will have a padlock symbol at the bottom of the page and a URL that begins with "https" instead of "http."
- **Verify Online Security Certificates.** These certificates are used to indicate a site is secure. A certificate is what is behind the padlock symbol at the bottom of the page. If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will not have a certificate. If the certificate name does not match the site, do not use it and notify the institution.
- **If you use a wireless network, deploy proper encryption, password protection and secure firewalls.**
- **Be suspicious of requests for personal information.** Due to the increase of phishing and online scams, financial institutions have altered their practices and are unlikely to ask you for personal information in an email. Be especially cautious of "urgent" requests, as phishers try to excite or upset customers so they will react immediately.
- **Visit your financial institution's website online.** Most now carry detailed information about security safeguards, how to protect yourself against fraud, and how to get help should a problem occur.

FACTS AND MYTHS

Javelin Strategy and Research 2005

One of the latest and most comprehensive research studies, conducted by Javelin Strategy and Research by phone among 4,000 consumers, indicates that **online banking is much safer and more secure than most people think.**

The central – and counterintuitive – finding of the survey is that:

- **Identity theft is more prevalent offline with paper than online through use of a computer; and**
- Internet-related fraud problems are **less severe, less costly and not as widespread** as previously thought.

Other key findings include:

- **Watch your wallet.** The most frequently reported source of information used to commit fraud was a lost or stolen wallet or checkbook; computer crimes accounted for just 11.6 percent of all known-cause identity fraud in 2004 – and half these digitally-driven crimes stem from spyware, software the computer user unknowingly installs to make ads pop-up when the consumer is online.
- **Be careful who you trust.** Among cases where the perpetrator's identity is known, half of all identity fraud is committed by a friend, family member, relative, neighbor or in-home employee – someone known by the victim.
- **Keep your eyes open.** The majority of actual identity fraud crimes in the United States are self-detected. This reinforces the benefits of activity monitoring through electronic review of transactions, statements and credit reports allowing consumers to check their account activities quickly and efficiently – without waiting for a paper bill or statement. Victims of identity theft who detected the crime by monitoring accounts online experienced financial losses that were less than one-eighth of those who detected the crime via paper statements.

Online Risk: Facts & Fiction

Courtesy of Javelin Strategy & Research

Some consumers may be concerned about security when it comes to online banking and electronic bill pay, but Javelin's research shows that your risks of identity theft can actually be reduced by over 10 percent when you conduct your banking and bill payment online.

Your chances of becoming a fraud victim through online bill payment are less than the probability of being struck by lightning or dying from a poisonous plant or animal.

Still concerned?

- Your probability of being struck by lightning is 600,000 to one.
- Your probability of dying from a poisonous plant or animal is 700,000 to one.

Refer to the Javelin Strategy and Research's Myths and Facts to help clear up the confusion and set the record straight about the safety of online bill payment.

**JAVELIN STRATEGY AND RESEARCH'S MYTHS AND FACTS
ABOUT ONLINE SAFETY**

Myth:	Facts:
If I sign up for online banking, a hacker will be more likely to access my account.	Despite sensational headlines, hacking -- unauthorized access to an online account -- is almost unheard of among major financial institutions. With high security encryption, firewalls and other protective technologies used by the major financial institutions, a criminal would have a very difficult time getting access to an online account.
Most identity theft is caused by fraudsters who steal information from an online bank account.	Most people assume that total strangers -- criminals -- cause most fraud and identity theft. The opposite is true. Most fraud and identity theft happens "the old-fashioned way" -- from lost or stolen credit or ATM cards or when people give their passwords or PIN number to acquaintances, friends or family members. It's much easier to steal a wallet or purse than to get through a bank firewall.
When it comes to money, you're always safer using traditional paper statements and mail.	Handling confidential paper documents such as bank and credit card statements or personal checks can actually be riskier than being online. Any paper can be stolen from the U.S. Mail or directly from an individual's mailbox or trash bin. Paying bills and banking online, where personal information is transmitted electronically, is safer than paper copies sent through the mail.
If a thief wants to access my accounts there is not much I can do about it.	Just as people are trained to drive a car safely, consumers also need to learn the "Online Rules of the Road." When used properly, online banking and statement management can actually help prevent and detect fraud. Consumers who bank online can monitor their accounts 24/7 -- at their convenience -- and be better able to detect any suspicious activity early. In addition, consumers should also beware of emails requesting personal or financial information.
If fraudsters get access to my online bank accounts, I could lose all my money.	Most leading online financial institutions stand behind their online security with guarantees that they will cover a customer 100% if any funds are improperly removed. Consumers should make sure their financial institution has this guarantee.

Courtesy of Javelin Strategy and Research, reprinted with permission.

RESOURCES

BITS Resources

BITS E-Scams Papers (Members Only)

BITS Voluntary Guidelines for Fraud Reduction

BITS Security Awareness Critical Success Factors

Fraud Prevention Strategies for Internet Banking White Paper

Identity Theft Uniform Affidavit

Financial Identity Theft: Prevention and Consumer Assistance White Paper

BITS Website, www.bitsinfo.org

ITAC website: <http://www.identitytheftassistance.org/home/index.cfm>

Federal Resources

Federal Trade Commission <http://www.consumer.gov/idtheft/>

Department of Justice <http://www.usdoj.gov/criminal/fraud/idtheft.html>

U.S. Postal Inspection Service <http://www.usps.gov/postalinspectors/>

U.S. Secret Service <http://www.secretservice.gov/>

Federal Deposit Insurance Corporation <http://www.fdic.gov/consumers/>

Credit Reporting Bureaus

Equifax <http://www.equifax.com/>

Experian <http://www.experian.com/>

TransUnion Corporation <http://www.tuc.com/>