The Sky IS Falling: The Need for Stronger Consumer Online Banking Authentication

George Tubin
Senior Analyst

Apr 2005
Reference # V42:27N

Two Charles River Place
63 Kendrick Street
Needham, MA 02494
United States

T +1.781.292.5200
F +1.781.449.6982
towergroup.com

TowerGroup Take-Aways

- E-mail-based phishing attacks are morphing into a more insidious form of online fraud that must be dealt with by financial institutions.
- The new methods of online fraud utilize a variety of techniques, including spyware, browser hijackers, and remote administration tools.
- While industry defenses are effective against phishing, they do little to protect institutions and consumers against malware attacks on consumers' PCs, which do not require the user to manually divulge personal data.
- TowerGroup believes that the consumer desktop is highly vulnerable to malware attacks and urges banks to recognize the fact that consumers' credentials will become increasingly compromised over the Internet as well as other channels.
- In addition to the defenses implemented for e-mail phishing, TowerGroup recommends that the industry develop stronger authentication approaches to combat fraud and preserve consumer confidence in online banking.

Report Coverage

The proliferation of incidents and varieties of online fraud is a cause for alarm among online consumers. TowerGroup has shown that fraud losses associated with phishing are minimal relative to overall bank fraud losses: Direct phishing losses amounted to some $137 million (USD) in 2004. Nonetheless, consumers and banks are extremely concerned about Internet fraud, as well they should be. Online fraud is morphing from phishing (a social engineering attack) to more insidious and furtive methods. This TowerGroup Research Note discusses the emerging methods that criminals are exploiting over the Internet to compromise customer information with the intent of committing online fraud. The Note discusses stronger authentication approaches as a way to combat the growing risk of widespread customer credential theft. TowerGroup urges the industry to develop stronger authentication approaches to combat fraud and preserve consumer confidence in online banking.

Background

Authentication has come a long way. From simple handwritten signatures to official seals pressed into wax on sealed envelopes to advanced cryptography techniques used by the military and government agencies, authentication techniques seek to validate the authenticity of someone or something. Today more than ever, the rise in online fraud as one result of the anonymity of the Internet necessitates the use of strong authentication techniques.

The username/password login that has been the standard user identification since the inception of online banking put the onus on the user not to divulge personal information to anyone, deliberately or unwittingly. ("Anyone" includes immediate family members, who have been the most likely perpetrators of account theft crimes.) Following simple procedures such as not carrying one's username and password so they could not be stolen or closing a browser window after an online banking session served the industry well in preventing widespread online banking fraud. However, the industry did not foresee the evolution of Internet fraud techniques and their effects.

Cunning fraudsters put a new spin on an age-old confidence game with the technique known as phishing. The financial services industry quickly developed defenses against phishing attacks. However, these defenses are not infallible. Consumer education was one of the most effective techniques to avoid phishing attacks, but new mutations of the original phishing paradigm are making these attacks more difficult to defend against. More important, they are shifting the onus of protection for online banking. See TowerGroup Research Notes V41:10PCN, *A Phish Tale? Moving from Hype to Reality*, and V41:11PCN, *No Phishing Zone: Vendor and Industry Initiatives to Curb E-Mail Fraud*, for a more detailed examination of phishing and approaches used to combat this problem.

The typical phishing attack is social engineering because the consumers who are the targets are manipulated. They are tricked into divulging their usernames and passwords needed to access their online banking accounts or other e-commerce sites. With these credentials, the fraudster can skim funds, take over accounts, and steal the account holders' identity. 2004 saw a tremendous rise in phishing. Based on early indications, TowerGroup believes that 2005 will see a similar rise in stealth "malware," malicious payloads delivered to individuals' personal computers.

The newer attack techniques are of a different kind than classic phishing and require different defenses. Classic phishing depends on e-mail as the "attack vector," the method to gain access to individuals' computers. However, the new forms of attack, spyware, Trojan horses, and keyloggers, cause a user to unwittingly download malware, which is computer code developed for the malicious intention of collecting various user information. The stolen information can be used for identity theft, which is a much more insidious prospect than the account skimming or account takeover associated with the more common phishing attacks.

In the past several months, the rise in these new attacks has been astonishing. For example, Brazilian authorities arrested a crime ring in November 2004 for allegedly stealing $30 million from Internet bank accounts by sending out e-mails with Trojan horses capable of stealing users' passwords and security codes. In January 2005, police arrested a ring of 13 people for allegedly stealing $600,000 by using spoofed online advertisements and spam e-mails to install keyboard loggers on user PCs to steal username and password credentials. In February, a Bank of America corporate banking customer sued the bank after $90,000 was allegedly stolen from his account through the use of a keyboard logger.

While antivirus and antispyware programs serve to protect users from having malicious code installed on their PCs without their knowledge, these applications are seriously lacking in effectiveness and not widely adopted. A joint study conducted by America Online and the National Cyber Security Alliance found that 67% of survey respondents either had no antivirus protection or had not updated their protection within the past week. Even so, the velocity with which new attacks and attack vectors are emerging renders the antivirus software obsolete the moment it is deployed. Antivirus and antispyware applications continue to be effective against known attack approaches and somewhat effective against known system vulnerabilities (software design flaws that could be exploited for malicious purposes). However, criminals are constantly finding innovative ways to circumvent the antivirus and antispyware security applications. Exhibit 1 shows the rise in system vulnerabilities reported to the US Computer Emergency Readiness Team (US-CERT) Coordination Center over the past several years. The chart indicates a general rise in vulnerabilities across all software types, which includes those affecting the consumer desktop. Criminals exploit these vulnerabilities to gain access to systems and information.

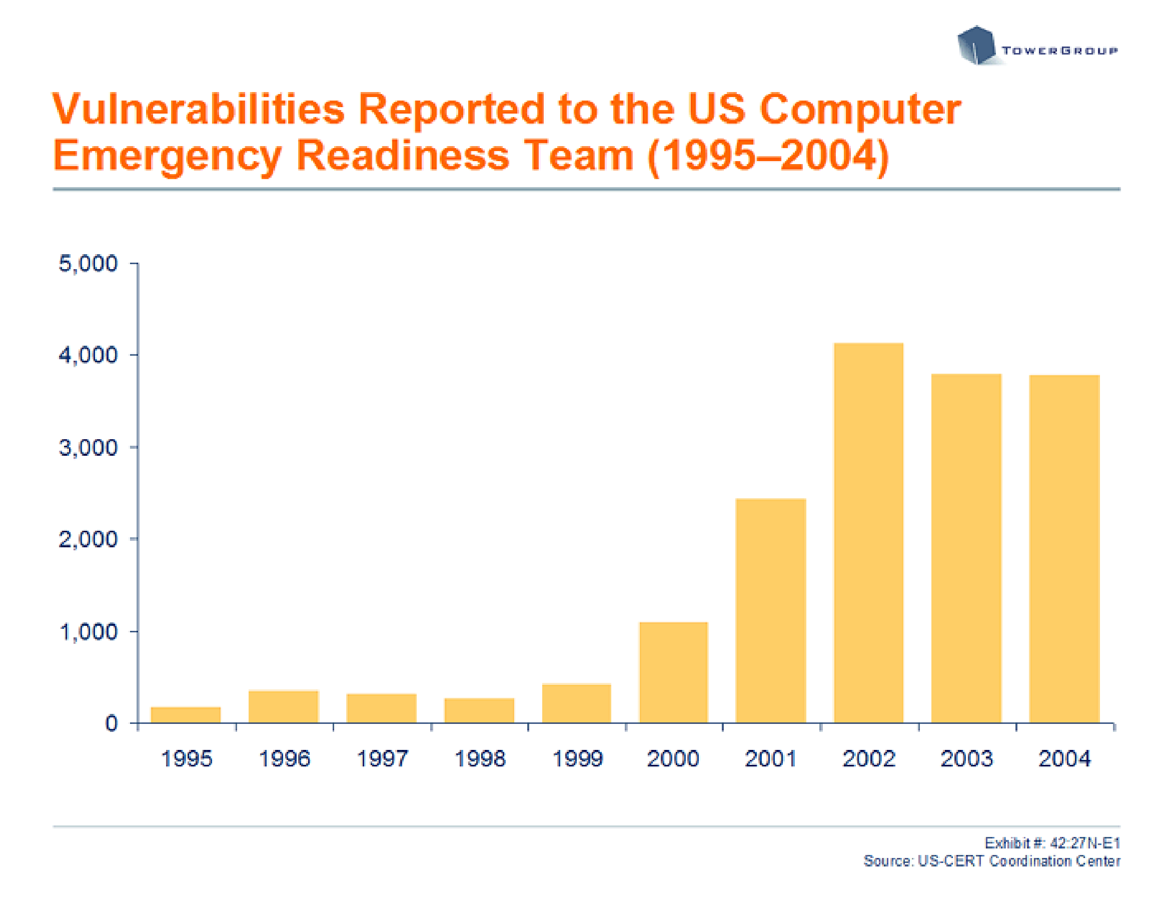


Exhibit 1
Vulnerabilities Reported to the US Computer Emergency Readiness Team (1995-2004)
Source: US-CERT Coordination Center

Financial institutions are clearly responsible for compromised data in their possession that results in fraud. Account holders have typically been held responsible for guarding against the theft of their banking information as well as any fraud perpetrated as a result of compromised credentials. While this continues to hold true in the traditional banking channels, banks have, for the most part, borne the responsibility for fraudulent activity perpetrated via the Internet channel. During the recent rise of phishing attacks, banks have reimbursed most customers for losses, although the customers clearly (albeit unwittingly) compromised their account credentials.

Knowing the relative ease of compromising the username and password, financial institutions must look to more effective techniques for authenticating online banking users. Most of the more advanced authentication technologies are well known but have been dismissed as being both too burdensome for the end user and the institution and too expensive for the institution to warrant their deployment. However, in light of the emerging online fraud techniques and their likelihood of rapid expansion, the industry must reassess the adoption of stronger authentication technologies or risk alienating a large swath of their current and future online customer base.

Deciding on an authentication solution is not simple and involves quite a few nuances. Consumer confidence is critical for the continued use and future adoption of e-commerce and online banking. While deploying stronger authentication will provide enhanced security and make most consumers feel more secure, some institutions fear that it may also send a message that the current username/password approach is deficient. If an institution only partially deploys a stronger authentication solution, how does the institution deal with consumers who do not adopt the solution? The institution may be held liable or at least perceived to be liable for not providing the same protections evenly across the entire customer base. It is likely that institutions that partially deploy stronger authentication technologies will have to provide different liability policies for adopters and nonadopters.

The Need for Stronger Authentication

Internet security and the potential for online fraud have been, and will continue to be, an ongoing concern for institutions, consumers, and government agencies. Its openness and anonymity make the Internet an environment that is ripe for fraud and deception. For institutions, the initial focus of Internet security was on their own corporate systems: ensuring that data was not compromised and that systems were not harmed. It was primarily in response to the advent of phishing that financial institutions focused their efforts on improving security for online banking consumer access. See TowerGroup Research Note V41:11PCN, *No Phishing Zone: Vendor and Industry Initiatives to Curb E-Mail Fraud*, for more information antiphishing solutions.

Internal security measures at financial institutions are generally considered to be sound. However, several senior security officers at financial services institutions (FSIs) have expressed a growing concern over the vulnerability of the consumer desktop, an area that is outside the banks' control. Financial institutions must consider the growing threats and develop approaches to protect consumers from online fraud.

Evolving Attack Vectors

With respect to computer systems, an attack vector is simply the method used to gain access to the device to deliver a malicious payload (malware). Hackers and fraudsters exploit systems by using attack vectors that most easily allow access to the system. An attack can use one or more vectors. Because defenses against attacks are eventually developed, criminals constantly seek to exploit systems through new attack vectors that are more vulnerable.

When criminals realized that a basic e-mail hoax could dupe users into providing sensitive online banking username and password information, the attack vector of e-mail deception, or phishing, became the attack vector of choice. Then, the fraudsters coupled e-mail hoaxes with imitated ("spoofed") Web sites, combining two forms of deception as a better way to dupe users into divulging personal information. Financial institutions quickly began educating their customers about this attack vector and implementing a variety of countermeasures that were effective in containing the phishing threat. Because making a dishonest buck through e-mail deception is becoming more difficult, the fraudsters have begun exploiting more vulnerable attack vectors.

New attack vectors will increasingly be exploited by online fraudsters to obtain access to consumer data to commit online fraud. Unlike the current form of phishing, the newer attack vectors will not require any action on the part of the user. It will just happen. While other attack vectors exist and new ones are being formulated, the following attack vectors demonstrate the increasingly clandestine methods that online fraudsters are using to deliver malicious payloads to the desktop.

Deception. Deceptive e-mail and Web sites trick the user into divulging personal information. This vector requires the user to type in personal information, whereas most other attack vectors do not require any action on the user's part. Deception is the essence of phishing.

E-mail Attachments. Although most Internet users are aware of the dangers of opening e-mail attachments, this attack vector continues to thrive. E-mail attachments are capable of containing various types of malware, including Trojan horses, viruses, spyware, and browser hijackers. When the e-mail attachment is opened, the payload is installed. The malware may also be hidden in a macro within a spreadsheet or document and executes when the file is opened.

Pop-Up Download. When a user visits a Web site, a pop-up window instructs the user to click on a button to do something seemingly helpful. The window may suggest that spyware has been found or that free emoticons are available and instructs a user to click on an offer that secretly downloads malware.

Drive-By Downloads. Internet browser vulnerabilities are exploited so that malware is automatically downloaded when a user visits a Web site, clicks on (what seems like) a navigation link, or reads an HTML e-mail message. This attack vector is especially dangerous because it can install the malware secretly without the user ever knowing what happened if the PC's security settings are sufficiently lax.

Hacking. Hackers have extensive knowledge of the workings of the Internet and can exploit security vulnerabilities to gain access to systems. Once inside, the hacker can do almost anything, including take over the computer completely. The hacker can improvise and try different approaches to breach a system's security, but hacking is inefficient because hackers typically focus on one system at a time. Instead, they often prefer to focus on the attack vectors that can reach the masses more efficiently.

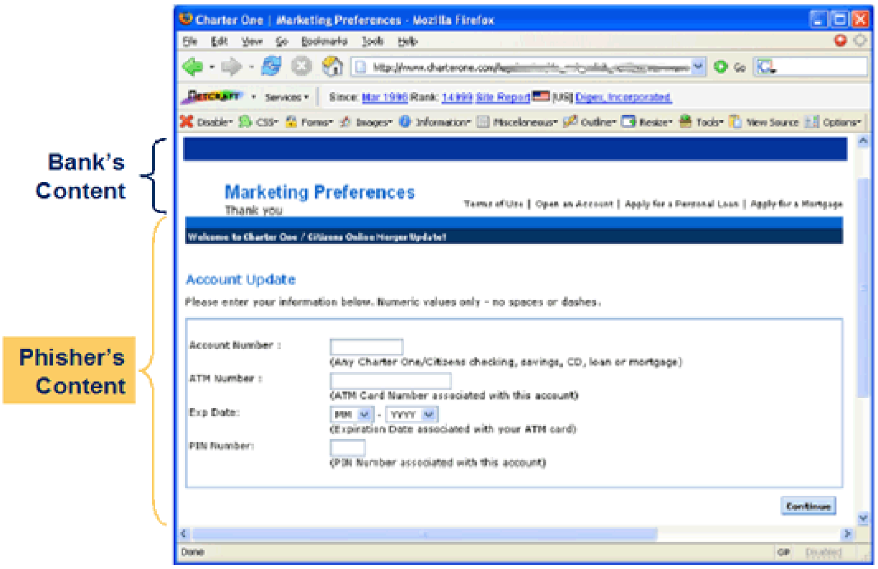
File-Sharing Networks. These peer-to-peer connected networks were designed for Internet users to share software and files (presumably legally). The danger in participating in these networks lies both in the file-sharing software itself and the shared software that is downloaded across the network.

Trojan Horses. While some argue that Trojan horses are a form of malware, others argue that these programs are actually attack vectors because they provide a means for malware to infiltrate a system. Like the Trojan horse of Greek mythology, this type of program gains entry under disguise. The program comes disguised as something that the user intends to download, but it actually contains malware that installs itself when the program is executed. For example, a user may download a free game or screensaver that looks appealing, only to launch malware instead of (or sometimes in conjunction with) the desired file. Although Trojan horses were once primarily associated with remote access tools, they now deliver other payloads as well, including spyware and browser hijackers (explained below).

Cross-Site Scripting. Fraudsters exploit Web site vulnerabilities to inject their own code into legitimate Web sites to serve up legitimate-looking content and frames within the legitimate Web site. Consumer login credentials can be stolen through legitimate-looking forms, or the user could be directed to a spoofed site. See Exhibit 2 for an example of cross-site scripting.

TowerGroup

An Example of Cross-Site Scripting


Bank's Content
Phisher's Content
File Edit View Go Bookmarks Tools Help
Go
Services
Disable CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Continue
Done

Charter One | Marketing Preferences - Mozilla Firefox

http://www.charterone.com/

Since: Mar 1996 Rank: 14999 Site Report [US] Digex, Incorporated

Marketing Preferences
Thank you

Terms of Use | Open an Account | Apply for a Personal Loan | Apply for a Mortgage

Welcome to Charter One / Citizens Online Merger Update!

Account Update

Please enter your information below. Numeric values only - no spaces or dashes.

Account Number : (Any Charter One/Citizens checking, savings, CD, loan or mortgage)

ATM Number : (ATM Card Number associated with this account)

Exp Date: MM - YYYY (Expiration Date associated with your ATM card)

PIN Number: (PIN Number associated with this account)

Exhibit #: 42:27N-E2
Source: Netcraft

Exhibit 2
An Example of Cross-Site Scripting
Source: Netcraft

Malicious Payloads

The payload delivered via the attack vector is ultimately focused on compromising the user's system in one way or another. While some viruses are simply created to wreak havoc, the payloads of concern here are those that allow criminals to secretly collect personal data to perpetrate fraud. These payloads can be installed through any one of the attack vectors described above or a combination and are usually undetectable by the average PC user.

Most people who have fallen prey to adware or spyware will admit that they do not know how the malware got onto their PCs and that getting the software off the PCs was quite a challenge. Effective malware embeds itself secretly in the system in such a way that it is difficult to detect and remove. Although hundreds of vendors provide antivirus and antispyware applications, these applications work best at identifying and removing previously identified malware. New malware is designed to circumvent known cures, causing the antimalware developers to work constantly in a "catch-up" mode. Thus, these applications may or may not be effective at removing new threats. Often, by the time malware is detected and removed, the damage has already been done. Moreover, consumers typically do not run their antimalware applications often enough and do not install updates. Even the most effective antimalware application is useless if it is not frequently updated and run.

Generally, the following types of malicious payloads are used to gather personal information via the Internet.

Spyware. The term "spyware" generally refers to a number of malware types, including adware, keystroke loggers, screen loggers, and pop-up window generators. Adware, which is typically more of an annoyance to most Internet users than a serious security threat, generates links, pop-up advertisements, and desktop shortcuts. Sometimes these actions are linked with a tracking program that tries to match the ads with the user's online usage profile, and other times the ads are randomly generated. One way that adware can be particularly dangerous is in generating a pop-up window that spoofs a legitimate Web site to lure consumers into divulging their usernames and passwords.

Keystroke and screen logger applications are readily available over the Web and can be used for legal purposes, such as by a parent monitoring a child's online activities. However, these applications are often used for the illegal purpose of stealing a consumer's personal information to commit fraud. Loggers can simply record and transmit all computer activities or actually recognize activities that are financially related like those involving credit card numbers or online banking logins. These logging tools record data into a log file that is either transmitted automatically back to the developer or resides on the PC until the developer retrieves the data using a backdoor (basically, a security flaw). Additionally, spyware can potentially record files and cookies on a user's PC as well as install additional spyware applications.

Browser Hijacker. Browser hijackers modify the browser in some way to direct the end user to Web sites that the developer (or the developer's clients) desire. Typically, the hijacker changes the browser home page and adds sites to the bookmark folder. Because the hijacker also changes the system registry, the home page will revert back even after the user resets it. Most browser hijackers constitute a severe annoyance, especially when the user is directed to pornography sites or when unwanted links continually appear in the browser.

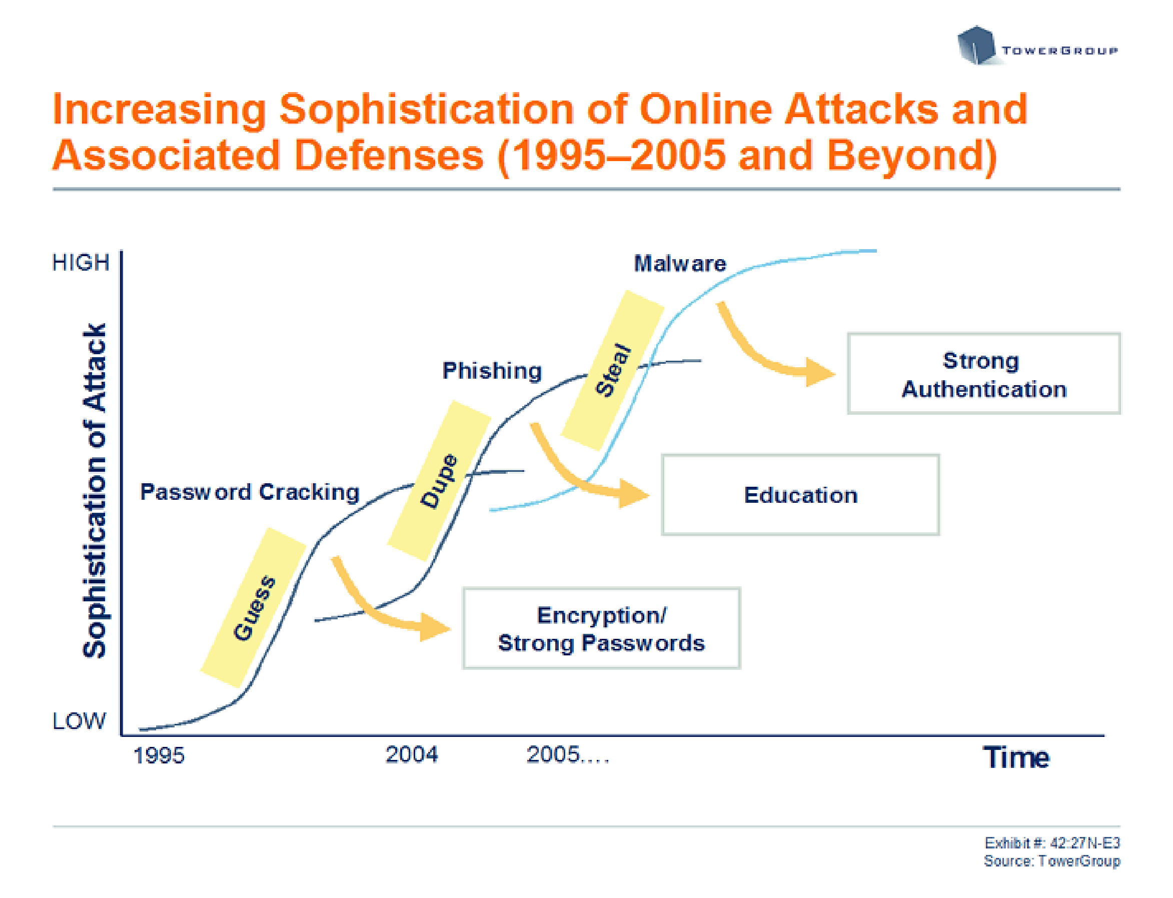
Much more dangerously, however, a hijacker can remap the system's host file, which links URLs to Internet Protocol (IP) addresses. Although this generally sends users to a sponsored Web site when they type in a legitimate Web address, one can envision a much more perilous manifestation of this approach taking form. For example, a user may type in the URL "www.mybanksite.com," but the hijacked browser could redirect the request to the IP address associated with "www.spoofedsite.com." Unwitting users would then arrive at a spoofed Web site (a very close replica of the actual bank site) and unknowingly give away their login credentials. This approach is similar to phishing, where the user is lured to a spoofed site through a legitimate-looking e-mail. Even if the user follows his or her bank's instructions by opening a new browser window and manually typing in the bank's URL, the browser hijacker could redirect the request to a spoofed Web site.

Remote Administration Tools. Also known as RATs, these programs are typically delivered by means of a Trojan horse, tricking the user into downloading and executing the malicious program. A RAT program runs invisibly to the user, but its effects are devastating. These applications provide remote access and full administrator control to a remote third-party operator. Once inside, the hacker can do almost anything, including read passwords and e-mail, install other types of malware, and use the computer as a relay point to mask his identity.

Clandestine Vectors Plus Dangerous Payloads Equals Devastation

Combining increasingly sophisticated covert attack vectors with hidden software designed to steal sensitive information makes for one nasty problem. Coupled with the fact that average Internet users are not equipped to protect themselves from the increasingly sophisticated attacks outlined here, the problem becomes downright scary. Even the most technology-savvy consumers will be challenged to defend themselves against these evolving attacks no matter how aggressively banks educate consumers and encourage the use of antivirus and antispyware applications.

The industry has been battling online attacks since the beginning of online banking. At first, banks worried about online passwords being compromised through friends and family, password guessing via simple and sophisticated approaches, and password interception. Banks responded to these vulnerabilities by employing stronger passwords and deploying Secure Socket Layers 128-bit encryption. The rise in phishing in 2004 caused institutions to implement additional security measures, including aggressive consumer education and online brand protection applications. See TowerGroup Research Note V41:11PCN, *No Phishing Zone: Vendor and Industry Initiatives to Curb E-Mail Fraud*, for more information on antiphishing solutions. With early indicators showing a rise in malware attacks, banks will need to respond with other defenses, including stronger online authentication approaches. For more information on the various types of malicious software, see TowerGroup Research Note V37:11C, *Financial Services and the Internet-Based Financial Services and Fraud: Star Wars Go Online!* Exhibit 3 is a time line illustrating the increasing sophistication of online attacks and the primary defenses.



TowerGroup

Increasing Sophistication of Online Attacks and Associated Defenses (1995–2005 and Beyond)

Exhibit #: 42:27N-E3
Source: TowerGroup

Exhibit 3
Increasing Sophistication of Online Attacks and Associated Defenses (1995-2005 and Beyond)
Source: TowerGroup

During the recent spate of phishing attacks, the industry has done remarkably well at containing the threat and reimbursing consumers who fell prey to the phishers. However, these attacks are beginning to target smaller, unprepared institutions that will likely suffer higher loss rates than larger institutions, which are more technology advanced. Further, traditional phishing defenses that focus on e-mail attacks will be less effective against the new threats outlined above. If the industry does not recognize the danger of these future threats and take immediate action, the results could be devastating. Fraud losses could rise to unprecedented levels, and bank investigation teams could be overtaxed.

Jupiter Aligns with Mars

While the situation described above seems ominous, there is a light at the end of the tunnel. Fortunately for the financial services industry, we are at a point in time that is ripe for implementing a long-anticipated security measure that has, until now, been highly impractical for widespread use. Several factors are coming together that will facilitate the implementation and adoption of stronger online consumer authentication:

- **Phishing is morphing** and becoming more dangerous. See the discussion of attack vectors and payloads above.
- **Two-factor authentication is recommended** by the Federal Deposit Insurance Corporation. In a report entitled "Putting an End to Account-Hijacking Identity Theft," issued on December 14, 2004, the FDIC stated: "Financial institutions and government should consider a number of steps to reduce online fraud, including . . . upgrading existing password-based single-factor customer authentication systems to two-factor authentication." The industry should act quickly to cure its own ills before this suggestion becomes a requirement.
- **Costs are dropping** for stronger authorization techniques. The cost of hardware-based token authentication has continued to drop as there are more deployments across industries and more vendors providing the devices. Some of the two-factor authentication approaches now available do not require additional hardware deployment.
- **New authentication techniques are less intrusive,** and consumers may be more willing to accept them. Banks have strongly resisted burdening their customers with carrying a device for online authentication. Banks believe that their customers do not wish to carry such a device and would be inconvenienced if multiple institutions required carrying a separate device for authentication. However, some of the newer approaches will not require the deployment of additional hardware and others are almost completely transparent to the user.
- **Customers will accept security measures presented the right way.** The widespread publicity of phishing and other online security issues will continue to increase consumers' concerns about online security. Consumer awareness of this growing danger will make the acceptance of stronger authentication techniques more palpable. Offering two-factor authentication on a voluntary basis is a first step toward deploying a more comprehensive online authentication program and will be far better received than requiring customers to accept a solution.

Authentication Options

Financial institutions have traditionally viewed the choice between advanced authentication approaches as selecting the "least bad" option. While stronger authentication does improve security, it has the potential to be costly, intrusive, burdensome, and imperfect. Online security and authentication are essentially exercises in risk management. A completely fail-safe solution would likely be cost prohibitive and resisted by consumers. An uncomplicated solution (like the typical ATM card and personal identification number, or PIN, used by many US banks for online banking authentication) is affordable and widely accepted but is prone to failure. Fortunately, the security industry has made strides in developing authentication solutions that are affordable, easy to use (or easier to use than previous methods), and reliable.

By now, most readers are familiar with the three types of authentication credentials available:

- Something the user knows (e.g., a password)
- Something the users has (e.g., a secure ID token)
- Something the user is (e.g., a biometric identifier)

Single-Factor Authentication

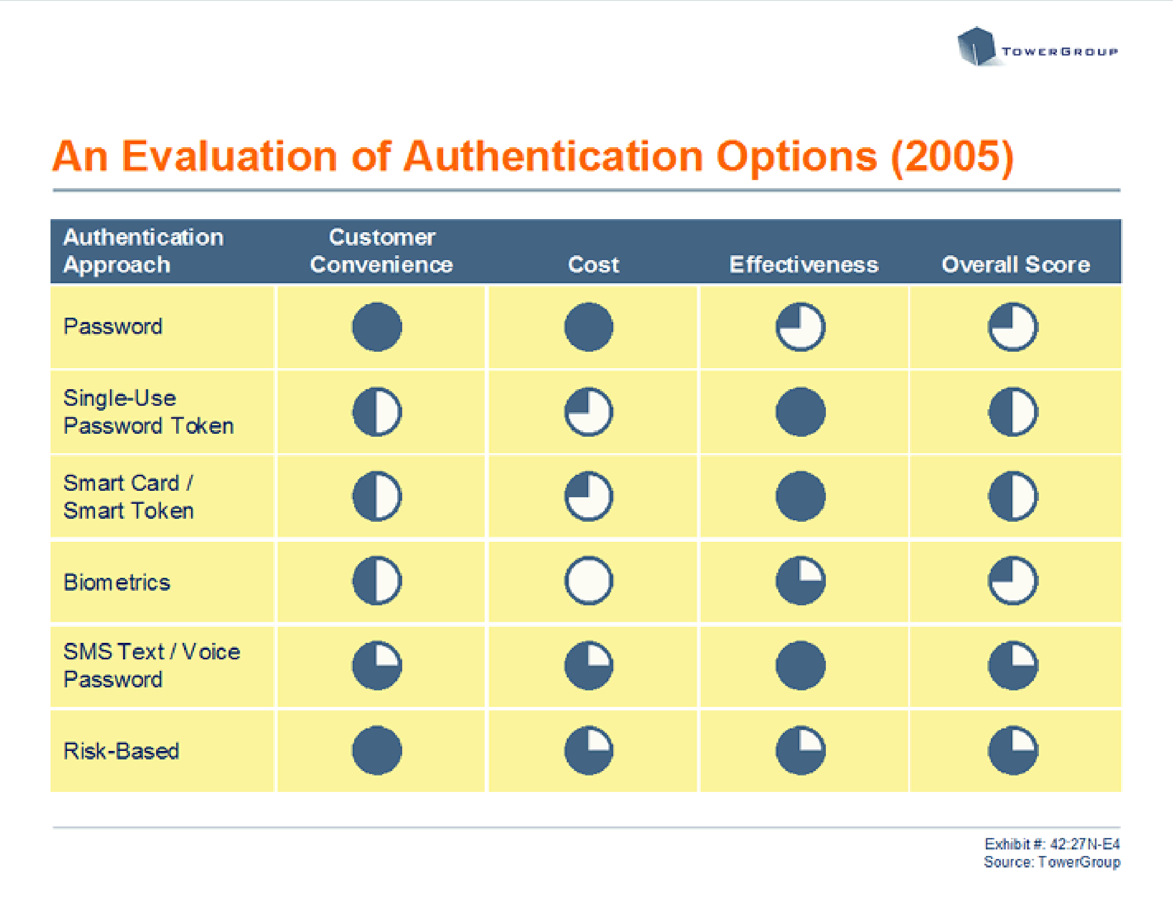
Currently, the most widespread approach for online banking single-factor authentication is the password, representing something the user knows. While this approach has the distinct advantage of being very easy to use and administer, it lacks the ability to combat the emerging fraud approaches outlined above. As we have seen, users easily can be fooled into divulging username and password combinations through phishing attacks, or these credentials can be stolen from the user's PC without the user's knowledge. Some banks have tried to strengthen such authentication by moving away from using the debit card number as the username and using the PIN as the online banking password, instead using unique usernames and alphanumeric passwords. This helps to improve security only marginally, however, because a twelve-character, case-sensitive, alphanumeric password can be stolen online as easily as a standard four-digit password.

Given that usernames and passwords are becoming more readily compromised over the Internet, TowerGroup believes that using only the traditional single-factor approach is an entirely deficient means of online banking authentication. The relative ease with which this information can be compromised should signal the need for a change in the industry's approach to online authentication. The password has served us well, but now it is time to move forward.

Two-Factor Authentication

Adding a second factor, something you have or something you are, as a requirement for authentication increases security well beyond the traditional single-factor approach because it requires the criminal to gain possession of both authentication factors somehow to commit fraud. Possessing a second factor usually means that some type of hardware authentication token must be present, along with the secret password, for the authentication to be successful. If a password is compromised online, it will be of no use without the hardware token. If the hardware token is lost, it will be of no use without the password. This approach is not foolproof, however, especially against the most common perpetrators of this type of fraud: friends and family. But two-factor authentication is a vast improvement over single-factor authentication.

The problems with two-factor authentication using hardware devices are well known. These devices add costs for the financial institution, including costs for the hardware and replacements, administration, and education. Most large consumer banks are fearful that their convenience-oriented customer base will reject the additional burden of physical tokens and may get overwhelmed with devices from several financial institutions. However, as the threat of online fraud rises, two-factor solutions become an easier pill to swallow. See Exhibit 4 for a comparison of authentication options.



TowerGroup

An Evaluation of Authentication Options (2005)

Authentication Approach	Customer Convenience	Cost	Effectiveness	Overall Score
Password	●	●	◔	◔
Single-Use Password Token	◑	◔	●	◑
Smart Card / Smart Token	◑	◔	●	◑
Biometrics	◑	○	◕	◔
SMS Text / Voice Password	◕	◕	●	◕
Risk-Based	●	◕	◕	◕

Exhibit #: 42:27N-E4
Source: TowerGroup

Exhibit 4
An Evaluation of Authentication Options (2005)
Source: TowerGroup

Single-Use-Password Tokens. The most common form of this solution is a small keychain fob that displays a six-character password that changes every 60 seconds. Many banks are using this type of solution to control remote employee access and as a stronger authentication solution for large corporate banking clients. The devices are available from a variety of vendors, including ActivCard, Aladdin, Authenex, Secure Computing, RSA Security, Vasco, and Verisign.

E*Trade recently announced that it had adopted a single-use-password token branded Secure ID (see Exhibit 5). The device is available on a voluntary basis and at no cost to Power E*Trade customers (who execute more than 15 trades per quarter) and to Priority E*Trade customers (who have over $50,000 in combined assets). E*Trade views the devices as a marketing opportunity, a way to demonstrate their security leadership and customer advocacy. The company believed there was a need to come to market with a stronger authentication solution due to customers' concerns over the rise in online fraud. This solution will likely be viewed quite favorably by the customer segments targeted by the firm.

Example of a Single-Use-Password Token: E*Trade's Secure ID Device

Exhibit #: 42:27N-E5
Source: E*Trade

Exhibit 5
Example of a Single-Use-Password Token: E*Trade's Secure ID Device
Source: E*Trade

Smart Cards and Smart Tokens. These devices contain computer chips that store information and perform basic computer functions. Smart cards are devices the size of credit cards, and smart tokens are akin to the small Universal Serial Bus (USB) storage devices that attach to key chains. The information stored on the smart device is protected by a PIN, ensuring that sensitive data is protected.

In addition to the problems associated with hardware devices in general, smart devices generally require some type of reader to interface with the smart device. Tokens can be read by the USB ports available on most newer PCs. However, readers are still necessary because such USB ports are not yet ubiquitous. Emerging smart card solutions include keypads and displays embedded into the card.

TowerGroup believes that FSIs must implement an alternative solution in the near term rather than wait for an industry-wide smart card authentication solution, which may not be available in the next five years. At some point, common smart devices will live up to their promise and provide multipurpose functionality, including strong authentication, healthcare information, stored value, mobile phone identification, and a host of other functions. Until that time, look for a more practical authentication alternative.

Biometrics. Too many problems continue to plague the biometric approach to authentication to make it a viable alternative as yet. Biometrics authenticate identity by means of physical characteristics, such as fingerprint, voice, retina scan, signature analysis, or keyboard cadence.

The expense and reliability of biometrics continue to be stumbling blocks. Authentication characteristics can be compromised, and once a biometric characteristic is stolen, it cannot be changed. The use of biometrics for online authentication is still some time away.

SMS Text Password. The use of Short Message Service (SMS) messaging for authentication requires a second, registered physical device: a cellular phone. At the time of authentication, a computer-generated code is sent to the user's mobile phone. Entering the code proves that the device is present and authenticates the user. This approach was implemented by ASB Bank of Australia in December 2004 and is being planned for launch by National Australia Bank, both on a voluntary basis.

Assuming the bank's customer base has a high percentage of cellular phone usage and is not opposed to the marginal SMS messaging expense, this approach provides a vast improvement over the single password. By using cell phones, a bank avoids the significant costs associated with hardware tokens, though it still must invest in the SMS messaging system and administration. And this method of authentication does not burden the user with a second authentication device as most methods employing hardware tokens do. Given a consumer base with high cell phone penetration, this approach is more appealing than most other hardware-based authentication schemes.

This approach could just as well send an automated voice message to a cellular or land-based telephone. Using automated speech technology, the customer would answer the phone to hear a short, one-time pass code for use in the current online authentication session. Vendors of outbound-alert technology could easily repurpose it for an authentication application.

Risk-Based Authentication. An emerging solution in the authentication space is a technique known as risk-based authentication. The way risk-based authentication works is to use the traditional username and password for login but at the same time analyze a variety of factors to determine the likelihood of the user being legitimate. Some of the Internet-related factors examined include data mined from the HTTP header and IP address of the server connection. This approach requires no additional burden on the part of the consumer (no cards or tokens to carry) and has proven, albeit in its very early stages, to be effective. Because the IP location is known, this is one of the few approaches that defend effectively against the "man in the middle" attack, where a fraudster acts as a conduit between the user and online banking site, intercepting all correspondence between the client and host and potentially taking over the session to commit fraud.

Risk-based authentication solutions will, at worst, offer an interim authentication solution for banks that are not prepared to implement hardware tokens but do not want to wait for the adoption of a "silver bullet" federated authentication approach. In the best case, risk-based authentication solutions will prove themselves to be highly effective at combating fraud while providing far less disruption to consumers than the token-based approaches. In a forthcoming Research Note, TowerGroup will examine risk-based authentication and the vendors that provide applications to support this approach.

Other Approaches. Other approaches to two-factor authentication have been proposed or tested, but none yet seem to provide adequate protection at an affordable price. Approaches such as secure cookies, onscreen keyboards for PIN entry, authentication by selecting known images, scratch cards with single-use validation codes, and others are available to enhance online security, but they have not yet gained traction in the market. Some of the on-screen approaches are feared to be vulnerable to screen loggers, while cookie-based approaches are vulnerable to malware. There is sufficient interest in improving online authentication that better solutions will continue to emerge.

Recommended Actions for FSIs

Selecting the correct path to strengthen authentication is not straightforward. As previously mentioned, the selection becomes an exercise in risk management. Calculating the costs of implementing and administering stronger authentication against the savings in reduction of consumer fraud losses is simple compared to quantifying the potential impact to consumer convenience and confidence. Each institution must assess the risks associated with its unique market position and customer base. Besides the recommendations set forth in TowerGroup Research Note V41:11PCN, *No Phishing Zone: Vendor and Industry Initiatives to Curb E-Mail Fraud*, institutions should consider the following recommendations when formulating their strategy for stronger authentication:

- Consumer education remains a critical element of online security. Make consumers aware of steps they can take to minimize their risks of acquiring the various types of malware.
- Hardware-based token authentication systems must be voluntary. Imposing a single solution on the institution's customer base will surely result in high defection rates.
- Increased security must be "sold." Position enhanced authentication as a positive step and use token devices as a marketing tool that proves the bank's commitment to enhanced security.
- Implement strengthened authentication in a tiered approach. As a first step, banks should consider implementing additional authentication measures for higher-risk, higher-value transactions. For example, to view account balances may require the customer to enter a simple username and password, but to add a new bill payee or conduct a wire transfer may require additional authentication.
- Investigate the emerging risk-based authentication approaches as well as approaches that utilize SMS or phone messages. These approaches require no extra hardware expense and little change on the part of the end user.
- Stay involved with industry groups that are working to develop federated, cross-industry solutions to stay abreast of the latest security and authentication trends. This issue is much larger than any single institution can address and must be met with large-scale, cross-industry initiatives.
- Centralize identity management within the organization and include the oversight and coordination of efforts across all customer touch points. Managing customer access from a single point greatly improves the organization's ability to recognize and combat fraud.

Summary

The gauntlet has been thrown down. Criminals are developing new ways of stealing consumer data to perpetrate fraud, yet the industry is still using old defenses. The practice of requiring usernames and passwords as the sole means for online authentication is rapidly becoming outdated. Customers' data will be stolen, and the financial services industry must do something about it. Banks can deal with the problem now or risk more devastating consequences later.

Fortunately, stronger authentication technology is an effective weapon to combat the rising tide of consumer data theft. Stronger authentication offers additional means to validate users even if the customer's logon credentials are compromised. Increased consumer awareness of the need for higher levels of security coupled with lower-cost and more user-friendly authentication methods will allow banks to implement stronger security to combat new types of fraud more effectively.