FIFTH THIRD BANK

February 2010

Dear Fifth Third Client:

As your trusted financial partner, Fifth Third Bank is committed to the safekeeping of your sensitive financial information. As part of this commitment, we want to make you aware of current online threats and provide you with valuable information to help identify and guard against them.

The security landscape has changed dramatically in the last few years. Mere bragging rights no longer motivate computer hackers. Computer related fraud is now run like cash-generating business ventures. This change has had a dramatic impact on the complexity, sophistication, volume, and evolution of security threats.

Continued education and heightened awareness are critical to combating fraud. Fifth Third has developed this reference guide, *Understanding and Managing Today's Online Threats*, to help you and your staff stay informed about what to look out for and best practices for protecting your sensitive information and business assets. The guide was created to serve as a reference tool for all Fifth Third Bank Commercial and Business Banking clients.

Security is an ongoing partnership between Fifth Third and our clients. We encourage you to read through and share the information contained in this guide. In the event you have any questions or comments, please contact your Fifth Third Bank Relationship Manager. We appreciate your business and attention to security details.

Table of Contents

Common Threats

Client Responsibility

Employee Resources

Security at Fifth Third Bank

Glossary / Resources

Phishing Scams

How Phishing Works

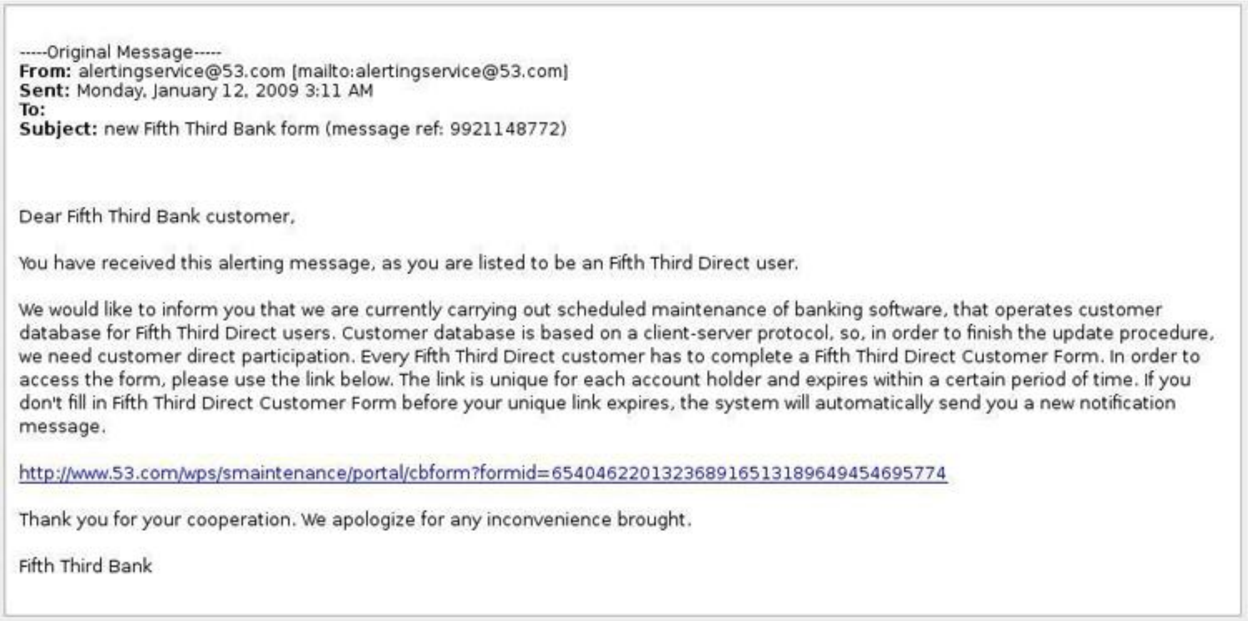
Phishing occurs when a fraudster impersonates a legitimate company or organization (this is the bait) using email, faxes, and/or Websites in an attempt to lure recipients into revealing confidential information. The messages are well crafted and often difficult to distinguish from those of the companies they impersonate.

A typical “phishing attack” begins with a fraudster sending thousands or millions of emails impersonating a company. Quite often the tone of the email is urgent leading recipients to believe there is something wrong with their account. They are urged to take immediate action, which often includes clicking on an embedded link to go to the “company’s” Website to update, verify, or review account information. Although the link may appear to be legitimate, computer code may direct the user to an imposter Website designed to be nearly indistinguishable from the legitimate site. When the victim logs in or enters confidential information, they are actually giving it directly to the criminals.

Phishers engage in these practices for pure financial gain. They like to impersonate financial services companies, Internet service providers (ISPs), and online retailers. The Internal Revenue Service has even been impersonated (typically during tax season) in the hopes of gaining Social Security numbers. Phishers have also pretended to be the Better Business Bureau, the Department of Justice, and PayPal, just to name a few. They are most interested in obtaining credit card numbers, online banking credentials, Social Security numbers, and other confidential information that will allow them or another criminal party to steal money, assume identities, and/or fraudulently apply for credit.

Phishing Examples

Here are some examples of phishing emails. Would they fool you?



-----Original Message-----
From: alertingservice@53.com [mailto:alertingservice@53.com]
Sent: Monday, January 12, 2009 3:11 AM
To:
Subject: new Fifth Third Bank form (message ref: 9921148772)

Dear Fifth Third Bank customer,

You have received this alerting message, as you are listed to be an Fifth Third Direct user.

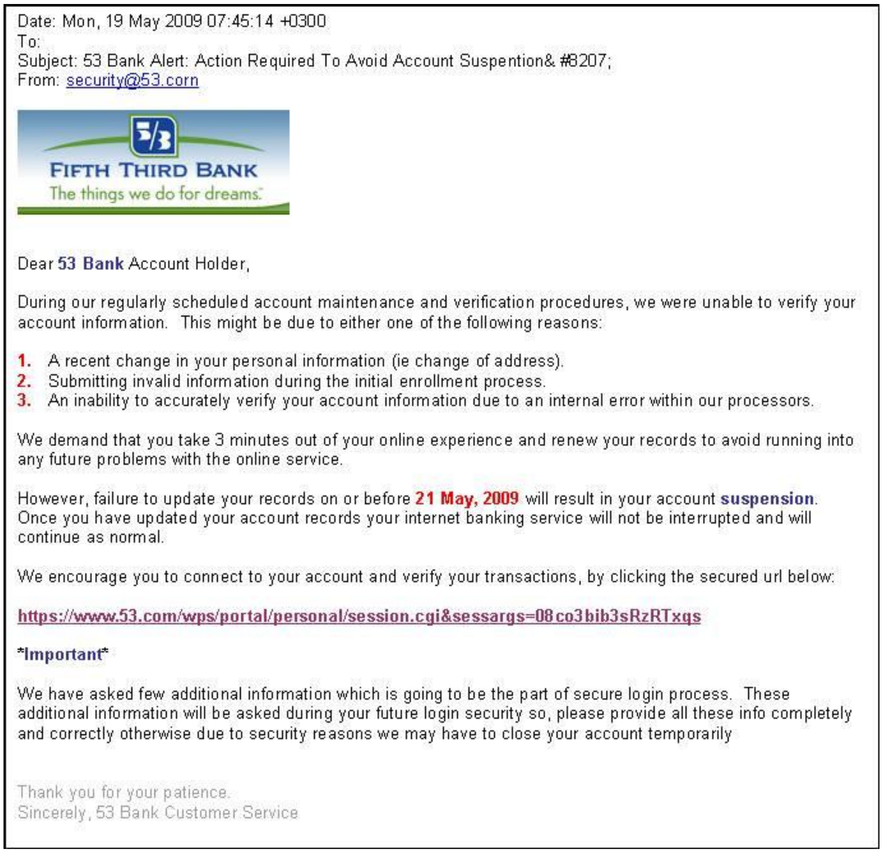
We would like to inform you that we are currently carrying out scheduled maintenance of banking software, that operates customer database for Fifth Third Direct users. Customer database is based on a client-server protocol, so, in order to finish the update procedure, we need customer direct participation. Every Fifth Third Direct customer has to complete a Fifth Third Direct Customer Form. In order to access the form, please use the link below. The link is unique for each account holder and expires within a certain period of time. If you don't fill in Fifth Third Direct Customer Form before your unique link expires, the system will automatically send you a new notification message.

http://www.53.com/wps/smaintenance/portal/cbform?formid=654046220132368916513189649454695774

Thank you for your cooperation. We apologize for any inconvenience brought.

Fifth Third Bank

Source: Fifth Third Bank



Date: Mon, 19 May 2009 07:45:14 +0300
To:
Subject: 53 Bank Alert: Action Required To Avoid Account Suspention& #8207;
From: security@53.corn

Dear **53 Bank** Account Holder,

During our regularly scheduled account maintenance and verification procedures, we were unable to verify your account information. This might be due to either one of the following reasons:

1. A recent change in your personal information (ie change of address).
2. Submitting invalid information during the initial enrollment process.
3. An inability to accurately verify your account information due to an internal error within our processors.

We demand that you take 3 minutes out of your online experience and renew your records to avoid running into any future problems with the online service.

However, failure to update your records on or before **21 May, 2009** will result in your account **suspension**. Once you have updated your account records your internet banking service will not be interrupted and will continue as normal.

We encourage you to connect to your account and verify your transactions, by clicking the secured url below:

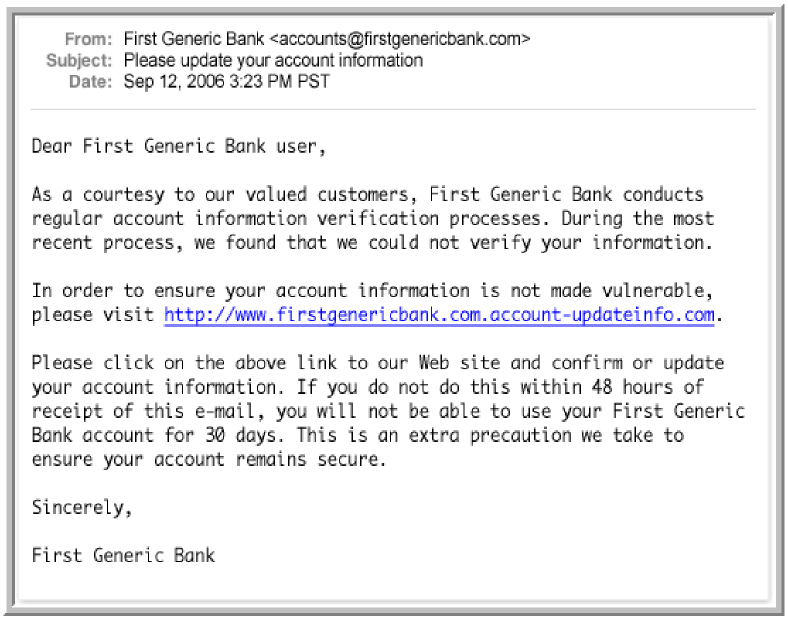
https://www.53.com/wps/portal/personal/session.cgi&sessargs=08co3bib3sRzRTxqs

Important

We have asked few additional information which is going to be the part of secure login process. These additional information will be asked during your future login security so, please provide all these info completely and correctly otherwise due to security reasons we may have to close your account temporarily

Thank you for your patience.
Sincerely, 53 Bank Customer Service

Source: Fifth Third Bank



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

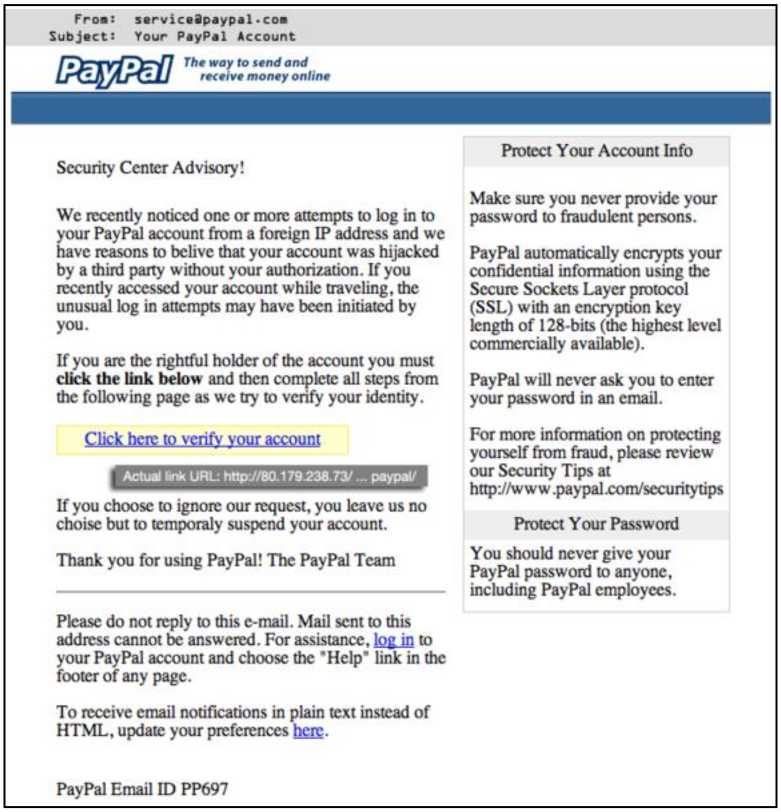
In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

Source: Phishtank.com



From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Source: Wikipedia.com

Common Signs of Phishing Emails

Although they are designed to be nearly impossible to distinguish from legitimate emails, there are some common signs you can look for.

- They urge the recipient to click on a link to update or verify account information.
- They convey a sense of urgency and often mention negative consequences for failing to respond.
- They do not contain any personalization; the recipient’s name, the last four digits of their account number or other information that shows that the sender knows something about the recipient’s account.
- They are unexpected and are not consistent with other emails from the company.
- They may contain spelling errors and bad grammar.

Phishers Are Smart

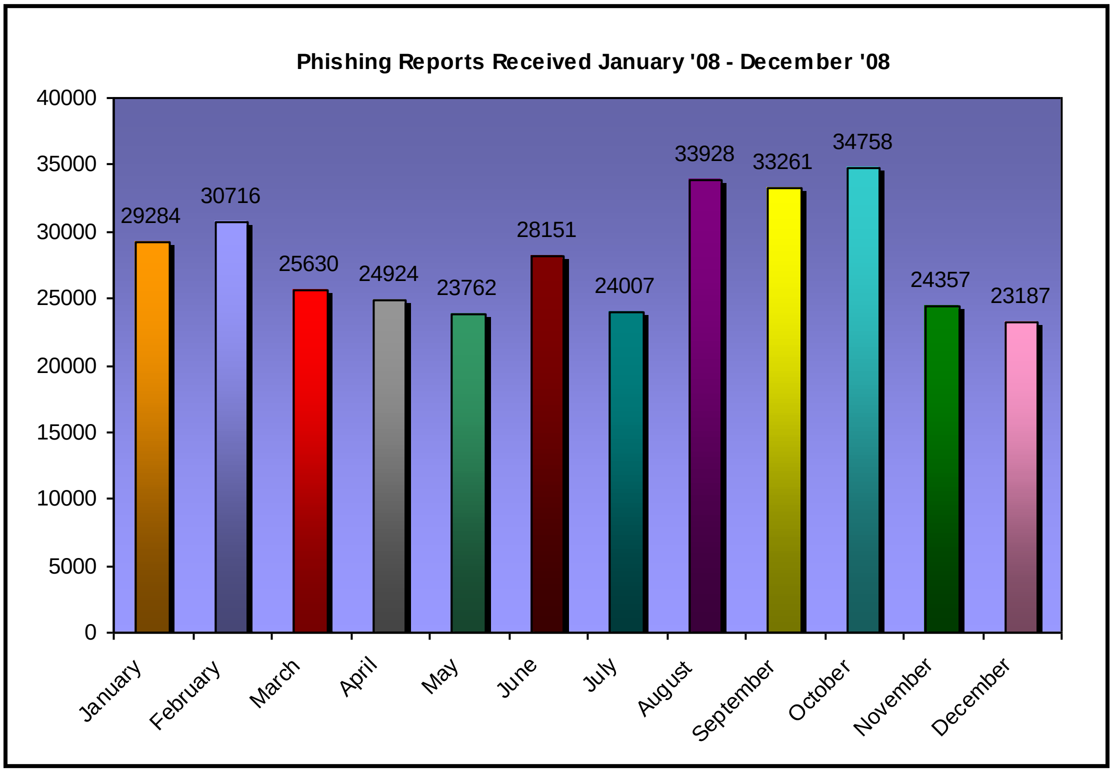
Phishers have learned to identify and capitalize on the fraud techniques that are most productive. Several factors have led to increases in phishing attacks:

- Attackers have learned to bypass email-filtering technologies by creating multiple randomized messages. This ensures that their message reaches more potential victims instead of being automatically deleted by email management systems.
- Using a large number of concurrent fraudulent Websites, they can sustain phishing attacks, making it more difficult for authorities to quickly track and disable the fake sites.

- According to Symantec Corporation, attackers have started sending a higher number of unique messages to more focused groups and individuals. For example, if the company being phished is an Australian bank, the attacker may limit the list of recipients to those with email addresses in the .au domain.
- Phishers are now leveraging social networking sites (e.g., MySpace, Facebook, LinkedIn) as good sources of potential victims. The information obtained can be used for identity theft or to gain access to corporate information and systems. Research indicates that phishing attacks on social networks have a success rate of over 70%!

How Prevalent Is Phishing?

Despite the decline of phishing reports received by the Anti-Phishing Working Group (APWG) in November and December of 2008, phishing is still quite prevalent, especially in the Financial Services sector. According to the APWG, financial services continues to be the most targeted industry at 92.4% of all phishing attacks recorded in January of 2008.



Information obtained from APWG Trend Reports

Phishing Damage

The damage resulting from phishing ranges from loss of email access to substantial financial ramifications and identity theft, which, according to a recent Javelin Strategy & Research Study, is now the fastest growing crime in America. Identity theft is becoming more popular because of the ease with which unsuspecting people divulge personal information. Once this information is acquired, the phishers have the vital personal information needed to create fake accounts, steal money or other assets, prevent victims from accessing their own accounts, or perform other types of fraud in a victim’s name.

According to a report from Gartner, during 2008 five million consumers in the United States lost money to phishing attacks. This is an increase of 40 percent over 2007. In another Gartner report, during a twelve-month period ending in August of 2007, victims of phishing scams in the United States lost $3.2 billion.

Vishing

Vishing is related to phishing in that the basic scam is the same. The fraudster is trying to trick you into divulging personal or financial information or to download malicious software. Vishing incorporates mass-distributed automated phone messages into the attacks. In this type of scam, special response phone numbers are used instead of fake emails and Websites. The term "vishing" is a combination of the words "voice" and "phishing".

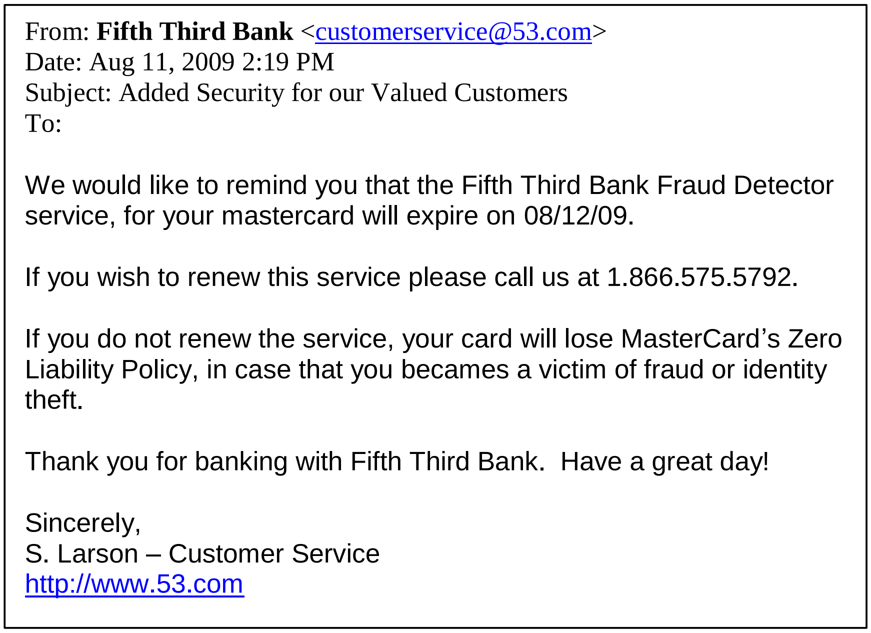
Vishing works as follows:

1. The criminal configures software to call phone numbers in a given region.
2. When the phone is answered, an automated recording is played to alert the consumer that their credit card account has had fraudulent activity, and the consumer should call the following phone number. The phone number could be a toll free number, often with a "spoofed" (fake) caller ID that displays the financial company they are pretending to represent.
3. When the consumer calls the number, it is answered by a computer-generated voice that tells the consumer they have reached account verification and instructs the consumer to enter their 16-digit credit card number.
4. Once the consumer enters their credit card number, the visher has all of the information necessary to place fraudulent charges on the consumer's card.
5. The call can then be used to harvest additional details such as a security PIN, expiration date, date of birth, bank account number, CVV number, etc.

Another twist to vishing includes emails similar to those used for phishing. The difference is that instead of asking you to click on a link, the email asks you to call a phone number to resolve the problem.

Vishing Email Examples

Here are some examples of vishing emails. Would they fool you?



From: **Fifth Third Bank** <customerservice@53.com>
Date: Aug 11, 2009 2:19 PM
Subject: Added Security for our Valued Customers
To:

We would like to remind you that the Fifth Third Bank Fraud Detector service, for your mastercard will expire on 08/12/09.

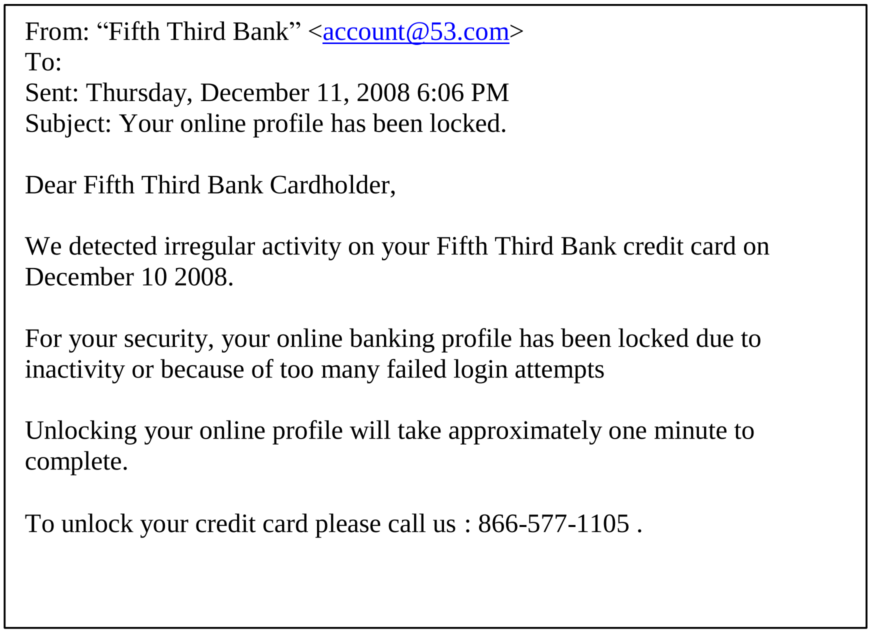
If you wish to renew this service please call us at 1.866.575.5792.

If you do not renew the service, your card will lose MasterCard's Zero Liability Policy, in case that you becames a victim of fraud or identity theft.

Thank you for banking with Fifth Third Bank. Have a great day!

Sincerely,
S. Larson – Customer Service
http://www.53.com

Source: Fifth Third Bank



From: "Fifth Third Bank" <account@53.com>
To:
Sent: Thursday, December 11, 2008 6:06 PM
Subject: Your online profile has been locked.

Dear Fifth Third Bank Cardholder,

We detected irregular activity on your Fifth Third Bank credit card on December 10 2008.

For your security, your online banking profile has been locked due to inactivity or because of too many failed login attempts

Unlocking your online profile will take approximately one minute to complete.

To unlock your credit card please call us : 866-577-1105 .

Source: Fifth Third Bank

SMiShing

The newest form of phishing is targeting cell phone and mobile device users. The term SMiShing is derived from a combination of the term “phishing” and “SMS” (Short Message Service), which is the technology used for sending text messages. Similar to phishing, SMiShing uses cell phone text messages to deliver the "bait" to get you to divulge your personal information. The "hook" (the method used to actually "capture" your information) in the text message may be a web site URL, however it has become more common to see a phone number that connects to an automated voice response system.

SMiShing works as follows:

1. The user receives a text message that requires their immediate attention and tells them to access a particular web site or call a specific phone number to address the problem.
2. An unsuspecting user may then go to the web site and end up downloading Malware or providing personal information, or the user may call the phone number in the text message and provide personal information such as an account number, social security number, user ID, password, and/or PIN to a person or to an automated service thinking they are talking to their financial institution.

In the Future

The Anti-Phishing Working Group, an industry and law enforcement association, has suggested that conventional phishing techniques could become obsolete in the future, as people are increasingly made aware of the social engineering techniques used by phishers. They propose that the use of Malware will become more common for stealing information.

Malware

Malware or “malicious software” is designed to infiltrate or damage a computer system without the owner’s knowledge or informed consent. Software is considered Malware based on the creator’s perceived intent rather than any particular features the software may include. The term Malware covers a host of software including computer viruses, worms, Trojan horses, spyware, and other malicious software.

The History of Malware

The first forms of Malware appeared in the late 1980’s and early 1990’s. They were computer viruses that were created as part of research, experiments, or pranks, and were generally intended to be harmless or merely annoying. Only a very small percentage of these programs were actually released “into the wild” where they could impact other computers.

In the early 1990’s, viruses began to be released to the wider population of computer users. Virus creators still worked individually, but advances in the Internet allowed them to meet online and share ideas. It was during this period that virus writers learned how to enable viruses to move between computers. Later, when Visual Basic became widely available, the editing of computer source code became much easier, and viruses proliferated. The sharing of infected Word and Excel documents became the most popular way to transmit viruses.

Soon Malware creators learned to create programs that could automatically replicate and transmit themselves to other computers within a computer network, and the computer worm was born. Viruses, which require human intervention to spread, and worms, which don’t, are still the best-known types of Malware, and these terms are often used interchangeably.

The Current Landscape

Malware is a significant problem. Malicious programs are now considered aggressive and sophisticated, often using a combination of techniques to accomplish their objective. Malware that combines exploitation of a flaw in operating system, browser software, or other applications (e.g., iTunes, Adobe, etc.) with viruses and other Malware is quickly growing in popularity.

Malware for personal digital assistants (PDAs), smart phones and other portable computer-based tools has now entered the market as well. As portable devices continue to grow in popularity, so too will this form of Malware.

Spyware, Trojan horses, and key loggers are becoming increasingly popular with criminals, including organized crime. These programs can be used to obtain confidential information about the user of the infected computer, such as account numbers and PINs, login credentials, the contents of email, even Internet habits, and the resulting data can easily be sold or used directly to perpetrate fraud. The following pages discuss these and other types of security threats in more detail.

As a result of Malware, users may find that their computers have become part of a botnet. A botnet is a collection of software robots, or bots, that run autonomously and automatically. While the term "botnet" can be used to refer to any group of bots, this word is generally used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed via worms, Trojan horses, or backdoors, under a common command-and-control infrastructure. If you take the necessary steps to limit your exposure to Malware, your computer will be less likely to become part of a botnet.

Types of Malware

There are many types of Malware, and they vary in their maliciousness. The table below summarizes the major types from least to most harmful.

Malware	Description	Risk
Misuse of Cookies	Cookies are pieces of information that are generated by a Web server and stored on the user's computer. The information they contain makes it easier for the user and the Website software if the user returns to that Website in the future. Cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences and the contents of their electronic shopping carts.	A convenience aid but can be read by other Malware
Adware	Adware or advertising-supported software automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while a specific application is being used. It is usually integrated into or bundled with a legitimate program as a way to recover programming development costs, and in some cases it may allow the legitimate program to be provided to the user free of charge or at a reduced price.	Nuisance, but potentially dangerous
Spyware	Spyware is a type of Malware that hides on your computer and gathers information about you and your Internet habits. The software then relays this information to advertisers, marketing groups, and others for advertising or malicious purposes. Information that is commonly collected includes login IDs, passwords, account information, surfing habits, shopping habits, and computer files. Spyware is usually installed without your knowledge when you download legitimate software. Sometimes the fine print of the license agreement includes information about the spyware component, but not always. For example, when installing certain freeware like weather monitoring software or file sharing software you may also install spyware applications on your system.	Dangerous
Trojans	Trojan, or trojan horse, software is malicious code that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. Trojans can be either • Useful software that has been corrupted by insertion of malicious code that executes the first time or every time the legitimate program is used. Examples of this type of trojan include weather alerting programs, computer clock setting software, and peer to peer file sharing utilities that contain system monitors or other Malware; or • A program that masquerades as something else, like a game or an image file, in order to trick the user into taking specific action necessary to carry out the program's objectives. Unlike some other forms of Malware, like viruses and worms,	Dangerous

Malware	Description	Risk
	trojans cannot operate autonomously. Trojans rely on the intended victim taking certain action to install and activate the programs.	
System Monitors such as Key Loggers	These programs range in capabilities and may record some or all of the following information: keystrokes, emails, chat room conversations, instant messages, Websites visited, programs run, time spent on Websites or using programs, and usernames and passwords. Unbeknownst to the victim, these programs transmit the collected or tracked information to or store it for remote retrieval by a third party. A key logger is a type of Malware monitoring software used by hackers to get information from your computer. Software or a physical device can be installed on your computer to track the information you enter using your keyboard. Key loggers copy keystrokes when passwords, credit card numbers, or other information that may be useful to the creator is entered. This is then transmitted to the Malware creator automatically, enabling credit card fraud, theft of funds, and other frauds. Some wireless keyboards also transmit your keystrokes and can be picked up surreptitiously by other users. Key loggers are a dangerous and growing type of system monitor, the most harmful type of spyware. Key logging software can be installed on your computer in many ways. • You can inadvertently download these malicious programs from the Internet by accessing a compromised Website or when downloading and installing infected software. • Some viruses deposit key logging programs onto your system. • You can become infected with a key logger from opening an infected email attachment. • If someone had access to your computer they could also install a software program that would monitor your keystrokes. Installation of a hardware key-logging device requires physical access to your computer. In this scenario a device is installed to your system, usually between your keyboard and your CPU.	Dangerous
Viruses	Software capable of causing great harm to files or other programs on a computer. Viruses cannot spread from computer to computer on their own; they usually access new victims through infected email attachments. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer. Some signs that may indicate your computer is infected with a virus include: • It is operating much slower than normal or getting hung up • You suddenly start seeing pop-up advertisements • You see a new home page	Dangerous

Malware	Description	Risk
Worms	A self-replicating computer program that uses a computer network or email to send copies of itself to other computers without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always harm the network (if only by consuming bandwidth), whereas viruses almost always infect or corrupt files on a targeted computer. Worms very often exploit a security hole or vulnerability in a piece of software or the operating system.	Dangerous
Rootkits	A software system that consists of a program, or combination of several programs, designed to hide or obscure the fact that a system has been compromised. Contrary to what its name may imply, a rootkit does not grant a user administrator access, as it requires prior access to execute and tamper with system files and processes. An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker has installed, along with the presence of the rootkit. Access to the hardware, *e.g.*, the reset switch, is rarely required, as a rootkit is intended to seize control of the operating system. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms.	Dangerous

Similar Symptoms of Spyware and Viruses

- Computer instability; your operating system slows down or hangs up. Spyware runs in the background and consumes significant amounts of memory and CPU speed.
- Dramatically slow network speed
- Advertising pop-ups, including pornography, gambling, etc.
- New toolbars appearing in your Web browser
- A new homepage appearing when you open your browser

Difference Between Spyware & Viruses/Worms

- Viruses are intended to cause downtime and disruption. Spyware, on the other hand, is developed primarily for financial gain.
- Unlike viruses, newer variants of spyware are highly adept at remaining on systems they infect. With spyware, multiple files are typically installed, not just a single file as is typical with viruses.
- Spyware transmission and infection is not limited to e-mail. Infected Websites or downloadable files from the Internet are the more common methods of transmission.

The Prevalence of Malware

The potential for financial gain has caused a tremendous increase in the amount of Malware being transmitted to computer users across the globe. The statistics are staggering. According to the McAfee 2009 Threat Predictions Report, McAfee Avert Labs identified a little less than 358,000 pieces of Malware during a 15-year period; however, more than 135,000 of those were identified in 2007 alone. By March 2008, they had already identified more Malware than in all of 2007. In 2008, Avert Labs identified almost 1.5 million pieces of Malware, an average of 3,500 each day.

Protecting Your Company

While Fifth Third can help ensure the security of your accounts, you play a vital role in preventing and reporting unauthorized account activity. The computer security landscape has changed greatly and there are a number of steps you must take to protect your business from the threats discussed in the previous section.

The Fifth Third Bank team is committed to protecting our clients' confidential information but our clients must also play an active role in this effort.

1. Protect your computers from malicious programs by using anti-virus and anti-spyware software, as well as a firewall. Keep these programs up to date. If your company has one or more Internet sites, it is recommended that you incorporate intrusion detection and vulnerability management.
2. Ensure that your employees cannot override or circumvent security software.
3. Implement a policy of updating your operating system and security software on all computers, and assign someone the responsibility for seeing that this is done on a regular basis.
4. Turn off and remove services that are not needed on computers. Do any of your employees need to use CDs, DVDs, or USB devices? If not, disable these unprotected conduits into and out of your computer system.
5. Proxy your internet traffic to limit user access to malicious sites and to potentially block malicious software from communicating with a Trojan controller should malware make its way onto one of your company's computers.
6. Make sure employee computer profiles have the least privilege possible. Very few of your employees should need "Administrator access."
7. If you have employees who use laptops, consider implementing software that will determine if mobile devices have been infected before allowing them back onto your network.
8. Review your account balance online on a daily basis to identify fraudulent transactions as soon as possible.
9. Use a mail service that blocks or removes email file attachments that are commonly used to spread viruses, such as files that end in .VBS, .BAT, .EXE, .PIF, or .SCR.
10. Install a pop-up blocker on your system.
11. Establish a procedure that can be used by any employee if they think their computer may be infected. Make sure employees understand this procedure and the importance of using it.
12. Ensure that only approved company applications are deployed on your computers and be sure to keep them updated (patched).
13. Set rules about employee use of the Internet.
14. Never enter personal or customer-specific information (e.g., account numbers, social security numbers, passwords, user IDs, other login credentials, etc.) into a public computer (those located in hotels, airports, libraries, etc.).

15. Make sure all employees use good security habits. Develop a security awareness program that addresses the risks specific to your business and/or to the specific functions within your company. (See the following pages for ideas.) Update it to include any new risks that have developed and review it with your employees on a regular basis.
16. Consider adhering to a recent FBI alert that suggests small businesses may want to dedicate one computer, which is never used for reading email or surfing the web, to handle all online banking activity. Having a dedicated computer would reduce the chance of the computer being infected with malware.

Detecting Spyware FAQ

How can I tell if my computer has spyware running on it?

By design, spyware is difficult to detect. In most cases, the creator of the spyware program does not want the victim to know that the spyware exists. Each piece of spyware is somewhat different, which makes it difficult to make a list of definite signs. In light of this difficulty, here are some things you may notice:

- Additional toolbars added to your web browser that you did not authorize.
- Pop-up windows that advertise services that you did not request.
- Unusual “windows” that show up and possibly go away when you start your computer or are browsing the Internet.
- Unusual links showing up in web pages where there are not usually links. These links will probably lead to web pages advertising some service.
- An unusual slow down in your computer’s performance.
- The appearance of unexpected programs in your computer’s startup folder.

Is there any software that can help me determine if I’ve been infected with spyware?

There are software packages that can detect and usually prevent spyware from being installed on your system. Some of these programs are part of a larger anti-spyware/anti-virus or Internet security package, and some are specifically designed just for spyware. To learn more about anti-spyware packages and how they stack up, visit www.pcmag.com or www.zdnet.com and search for “anti-spyware”.

To be effective, these programs must be kept up-to-date with the latest information about known spyware programs. Spyware is created daily, so anti-spyware software needs to be updated as often as possible.

New versions of popular web browsers, such as Internet Explorer 8.0 from Microsoft and Firefox 3.0 from Mozilla, include enhanced security features that help prevent spyware programs from attaching themselves to a user’s web browsers. Both of these popular web browsers also contain a feature to detect phishing / malicious software hosting Websites. The browser will alert the user when they have visited a known “bad” Website and give the user the opportunity to navigate away from the “bad” site before they have a chance to interact with it, or the browser will alert the user when they attempt to visit a Website or download software that is not considered safe.

Is there a guaranteed way to determine if I’ve been infected with spyware?

You should have any computer you suspect of being infected examined by a computer forensic examiner. These professionals are trained in special techniques and have tools designed to discover hidden programs, so they will be better able to tell you if spyware is present on your computer and, if so, what it was most likely doing.

If I want to have a computer forensic investigation done on my computer, where can I find a trained professional in my area?

Several sources for finding a computer professional certified for forensic examinations are:

- Your local police department
- Your local FBI office
- Your attorney (attorneys use computer forensics experts for various types of cases)
- Your accountant (accounting firms sometimes use computer forensic experts to validate accounting data)

Should I use my computer if I think that spyware has been installed on it? What if I actually discover spyware running on my computer?

If you suspect that your computer has been infected by spyware, you should avoid using it for any private or personal transactions. Contact a computer professional as soon as possible to have your computer cleaned of all malicious programs. Some spyware downloads other pieces of spyware once it installs itself on a victim's computer. If you find one piece of spyware, there is a good chance that there is more hiding in other places. Security is like a chain; it's only as strong as its weakest link.

Heightened Security Awareness

In these days of widespread information and technology use, individual computer users present the number one threat to information security. According to The Computing Technology Industry Association, human error is the primary cause of nearly two-thirds of reported security breaches. A security breach can be as simple and as commonplace as an employee allowing their computer to become infected with Malware by opening an unknown email attachment. Operating systems can be hardened, virus scans can be conducted, and hardware can be physically secured; however, if employees do not understand and embrace basic security best practices, these efforts would be wasted.

It is important to note that the risk of a security breach increases significantly when any of the following scenarios is present. How many of these scenarios exist in your company?

- The organization is involved in a highly competitive business.
- A terminated employee holds a grudge.
- Individuals in the organization lack security awareness and knowledge of best practices.
- Employees have laptops or access their files from a home computer system.

Who is responsible for security at your company? Every one of your employees is. People will not become aware and adopt good security practices on their own. They need to be coached and trained in order to understand what they should do.

People tend to resist developing good security habits, mainly because it is easier not to. Talk with your employees on a regular basis to let them know how important security is to your organization. It is especially important that those who are new to the company be given training on security best practices, so they can build good habits from day one. Employees are more likely to embrace good security practices if they understand that it is important to you and the risks the company could face if they don't.

The following pages contain information on security topics and best practices employees should be aware of.

THE FOLLOWING INFORMATION DOES NOT ADDRESS ALL SECURITY RISKS AND BEST PRACTICES AND THEREFORE SHOULD NOT BE USED AS A SOLE MEANS OF SECURITY TRAINING FOR YOUR EMPLOYEES.

Work with your technical resources to add discussion points about security issues, policies and practices specific to your company or function within your company. That way, your employees will recognize the role they play in protecting your organization.

Best Practices

Below are some security best practices all employees should understand and follow.

Don't …

- Try to disable or circumvent security software or procedures your company has put in place. They are there to help protect the results of all of your hard work and that of your co-workers.

- Tell anyone your passwords, user ID, or other login credentials.

- Enter personal or customer-specific information (e.g., account numbers, social security numbers, passwords, user IDs, other login credentials, etc.) into a public computer (those located in hotels, airports, libraries, etc.).

- View, open or execute any email attachment unless the attachment was expected and the purpose of the attachment is known.
  - This is the most common way computers become infected with key loggers and other malicious software (or "Malware").
  - Just because it appears to have come from someone you know doesn't mean it's not malicious. Some Malware is designed to send more Malware to the people in the infected computer's email contact list. Just by opening an unexpected attachment, you could cause your coworkers', friends' and family's computers to be one double-click away from getting infected!

- Allow anyone to access your computer without your knowledge. Keep your computer turned off or locked when you're not using it.

- Click "Agree", "OK", or "I accept" to get rid of a window such as a pop-up message or unexpected warning. Instead, close the window by clicking the red "X" in the upper-right corner of the window, or by pressing Alt + F4 on your keyboard.

Do

- Follow company security policies. They were developed in order to protect both you and the company.

- Be suspicious of ALL email. When you are requested to supply information via email, use a phone number you trust (NOT one in the email) to call the company, group or person from whom the request supposedly came. Verify that the request is legitimate before you give out any information.

- Be selective about what you install on your computer. Malicious programs can automatically be installed on a computer when installing other software.

- Carefully read all security warnings, license agreements, and privacy statements *before* you download any software. Language about unwanted software often appears at the end of the fine print. Make sure you clearly understand what you are getting into and that the benefits outweigh the possible costs.
  - Read the license agreement. Some spyware and adware can be installed after you accept an end-user license agreement or as a consequence of that acceptance.

    Learn what to look for at http://grc.com/oo/fineprint.htm.

  - Search the Internet for spyware reports. Use the software's name and the word 'spyware' as your search keywords.

- Know how to recognize computer hoaxes and phishing scams.
  - Hoaxes typically include a bogus warning to "send this to everyone you know" and/or improper technical jargon that is intended to frighten or mislead.
  - Phishing scams typically utilize emails with links to fraudulent Websites that entice recipients to divulge credit card or other confidential information.
  - Phishers have grown very good at impersonating legitimate companies. In fact, the emails and Websites they use are usually nearly impossible to discern from those of the company they are impersonating.
  - Understand that phishers don't just use email. They have also been known to try to collect information using automated phone messages and faxes, and are now using cell phone messages too.

- Know how to recognize the symptoms of infection. If you experience any of the following, your computer may be infected.
  - Your computer is slower than normal.
  - You are seeing more pop-up boxes than in the past. Many spyware programs track how people respond to these ads, and their presence is a red flag.
  - The page you automatically go to when you first access the Internet (your "home page") has been changed.
  - An unfamiliar search engine replaces your search engine.
  - A new toolbar appears at the top or bottom of your screen.
  - Your computer "crashes". This can even happen when your PC is turned on but you are not actually doing anything.

  If you experience any of these signs, run a scan of your computer to identify and disable any Malware or viruses on your system.

  You can be infected and not experience any of the common signs, so it is a good practice to scan your computer on a regular basis. Ask your technical resource whether your computers are automatically scanned. If not, ask him or her how you can scan your computer yourself and set a recurring appointment to remind you to run the scan.

- Always verify the identity and authorization of anyone who requests confidential information from you.
- IMMEDIATELY notify your manager and the company being impersonated if you feel you may have given out confidential information when you should not have.

  If the company involved is Fifth Third Bank, call Fifth Third's Customer Service professionals at 800-676-5869. They are available to serve you Monday through Friday from 7AM – 8PM ET and Saturday from 8:30AM – 5PM ET.

- Use strong passwords and protect them like the company secrets they are. (See the next page for details.)

Passwords: Your First Line of Defense

Your passwords are the key to protecting your computer and your sensitive information. Use strong passwords that are difficult to guess and protect them as if they were gold. In the case of your financial account passwords, that's exactly what they're protecting.

How Do I Create A Strong Password?

Each system or Website you use to access information will have different password requirements. When establishing or updating a password, keep the following tips in mind:

- The more variety there is in the characters used (numbers, upper and lower case letters, symbols), the more difficult it will be to guess the password.
- Similarly, the longer the password is, the more difficult it will be to crack or guess.
- It is very easy to crack passwords that are made up of a word or words that can be found in a dictionary (English or another language). It's also easy for hackers to substitute numbers for letters (such as "C1nc1nnat1" for "Cincinnati").
- You should not use easily obtained information for your password like the name of a pet or family member, an address, or current calendar month. Never use your date of birth, mother's maiden name, or Social Security number as your password.
- One easy way to create a strong password is to use the first letter of each word in a favorite phrase, song, or saying, inserting numbers, and a case change where possible. For example,

  TWObornot2b -- "To be or not to be."

  Wygc?GB1 -- "Who ya gonna call? Ghost Busters!"

  It is easy to choose a password that is both memorable to you and difficult for others to guess, you just have to use some creativity.

What Can I Do To Protect My Password?

Setting strong passwords is the first piece of armor in your computer defense arsenal. Once you have strong passwords in place, you need to protect them. If they were to fall into the wrong hands, much damage could be done.

- **Never** share your password with others at home or work.
- **Never** provide your password in an email or an unsolicited phone call.
- **Do not** write your password down. If you need a way to remember a password, write down a hint and keep it secure.
- **Do not** use the same password for all of the systems and Websites you access. Protect your most critical accounts and/or systems with special passwords.
- **Change the passwords of your most critical accounts/systems often.** Most companies recommend changing passwords every 30-60 days.
- **Never use the "save ID and password"** option on your computer.

Don’t Get Hooked By Phishing

What is phishing?

Phishing is an email scam used by criminals to conduct fraud. How do they do this?

1. They create an email that looks just like an email that a legitimate company might send.
2. They send this fake email encouraging you to click on a link in the email. If you click on the link, you will be taken to a Website that looks just like the legitimate company’s site.
3. Once at the fake Website you are asked to share, update, or confirm personal or financial information, such as your username, password, account number, Social Security number, etc.
4. The criminal(s) use this information or sell it to a third party who will use it to steal money, apply for and run up credit, or steal your identity.

This type of scam is called “phishing” because criminals use emails as a “lure” to entice recipients into “biting” by clicking on the link and revealing their confidential information.

Newer variations on the same theme include Vishing, which is phishing using the phone instead of a Website, and SMiShing, which is phishing using text messages. Although the technology used may be different, the scam is still the same. The criminals are still trying to trick you into divulging personal and/or financial information.

So, if you aren’t tricked into sharing any information, are you safe?

Not necessarily. Even if you don’t provide any of the requested information, simply clicking on the link in the email can cause unwanted software to be installed on your PC without your knowledge. These malicious pieces of software (called “Malware” for short) can track your keystrokes or monitor your activity and transmit the information they have collected about you to the criminals.

Do these scams always use fake email and fraudulent Websites?

No. Criminals know that they will increase the likelihood of getting people to respond by varying the approach and messages that they use, so they sometimes use automated phone messages or widely-distributed faxes asking recipients to call or fax their information to a special phone number. Scamming cell phone users via text messaging has also become popular, as more and more people are communicating this way.

How can you spot phishing emails, phone calls, and text messages?

Identifying which emails, phone calls and text messages are fraudulent and which are real can be tricky, because the fraudulent ones appear to be legitimate. If the email, call, or text message fits any of the following descriptions, BE SUSPICIOUS!

- You are urged to take action quickly.
- It contains one or more links.
- You weren’t expecting it.
- It asks that you verify, add or update information about your account.
- It simply urges you to log on and look at your account because there is a suspicion that something bad has happened to your account. It might say something like, “A recent

transaction appears to be fraudulent. Use this link or call this number to verify all recent transactions."

- It is not personalized in any way. It doesn't include your or your company's name, the last four digits of your account number, the name or phone number of your account contact, or anything else that would indicate the sender knows something about your specific account. The listing of a potentially fraudulent transaction doesn't count.

What should you do if you receive a potential phishing email?

- DON'T CLICK ON ANY LINKS OR CALL THE PHONE NUMBER PROVIDED. Forward the email to the company being impersonated, or "spoofed". Forward phishing emails that appear to come from Fifth Third Bank to 53investigation@security.53.com**.** Then delete them from your inbox.
- If you are unsure of its authenticity, call a phone number you trust such as one from your last statement, NOT the one from the email, to verify that the company actually sent it and why they need your information.

If you think you've provided sensitive information to a fraudulent Website or phone number imitating Fifth Third Bank:

- Call Fifth Third Customer Service at 800-676-5869. They are available to serve you Monday through Friday from 7AM – 8PM ET and Saturday from 8:30AM – 5PM ET.
- Visit the Federal Trade Commission's identity theft Website at www.consumer.gov/idtheft to learn how to minimize the risk to your identity.
- Contact your technical resources to notify them that your computer may be infected.

Remember:

- Legitimate businesses are aware of phishing and will not ask you to click a link in an email to access, update, or verify information about your account. Fifth Third will NEVER ask you to click on a link in an email to view, share, or update information about your account(s).
- Never click on a link in an email to go to a company's Website. Type the URL that you know into the Address field of your browser.
- Use hard-to-guess passwords that
    - Include as many characters as possible: numbers, upper- and lower-case letters, and symbols, if possible
    - Don't include words or names that could be found in any dictionary
    - Are different for different accounts

  One trick to setting strong passwords is to use one character or number to represent the first letter of each word in a favorite saying, song or quote.
- Change your passwords and PINs (for your credit and ATM cards) frequently.
- Monitor your account activity.

How to Protect Your Personal Accounts

Many of the steps you should take to protect yourself personally are the same as those for protecting your company.

1. Use the habits discussed in the Best Practices and Passwords section of this guide.
2. Protect your computers from malicious programs by using anti-virus and anti-spyware software and a firewall.
   - Make sure your anti-virus program scans both email and Instant Messaging attachments.
   - A good firewall hides your computer from hackers, gives you control over Internet traffic on your computer, and automatically blocks intruders.
3. Turn on the auto-update feature on your operating system and anti-virus and anti-spyware software, and be sure to update your applications to the most recent versions as well.
4. Scan your computer on a regular basis, even if you aren't seeing signs of infection. Many malicious programs are designed to sit quietly in the background, collecting and transmitting data, so you might never see direct signs of infection.
5. Don't use an Administrator profile for your every day computing. Any Malware you come in contact with will use the privileges associated with the profile you are currently using; if you have Administrator access, so does the Malware. You should, however, log into your computer using Administrator access once in a while to ensure all updates are being made, as some updates can only be completed when you are logged into your computer as the Administrator.
6. Keep your security settings high.
7. One way to avoid spyware is to take the following steps before downloading software onto your computer:
   - Read the license agreement. Learn what to look for at http://grc.com/oo/fineprint.htm.
   - Search the Internet for spyware reports. Use the software's name and the word 'spyware' as your search keywords.
8. Make sure everyone in your home understands and uses good security habits, knows how to recognize the signs of possible infection, and knows to not access financial and other sensitive accounts if they think their computer may be infected.
9. Never use the "save ID and password" option on your computer. Many Malware programs look specifically for stored passwords and User IDs on your computer.
10. Never click "Agree", "OK", or "I accept" to get rid of a pop-up message or unexpected warning. Instead, close the window by clicking the red "X" in the upper-right corner of the window, or by pressing Alt + F4 on your keyboard.
11. Shred documents that contain confidential information about you, a family member, or a financial account.
12. Put a hold on your mail while you are on vacation, and put any outgoing mail that contains confidential information or checks into a locked mailbox.

13. Memorize your PIN numbers. Don’t carry them in your wallet or purse.
14. Never give out your Social Security number over the Internet. If you get a request for it, verify the identity of the requestor and the reason why they need it and then provide it directly to that person.
15. Never use email, Instant Messaging, or text messages to communicate sensitive information. These mechanisms are not secure.
16. Use an email service that blocks spam.
17. Password-protect all your computers and personal digital assistants (“PDAs”). That way if you lose them or they are stolen it will be more difficult for whoever ends up with them to recover the information you’ve stored on them.
18. Before you sell or give away an old computer, remove the information that’s stored on the hard drive.
19. Minimize the amount of personal or financial information you store on your computer. There are certain types of Malware that are designed specifically to look for and transmit this kind of information.
20. Be careful when putting personal information onto a social networking site. These sites are prime sources of information for phishers and identity thieves.
21. Carefully review your banking, investment, and credit card statements each month. If you notice any unusual transactions, contact your financial services company immediately.
22. Check the credit reports for yourself and each member of your family on a regular basis. The three major credit reporting agencies, Experian, TransUnion, and Equifax, are each required by law to give you one free credit report each year.

    To order your free credit reports:

Log on to	www.annualcreditreport.com,
Call	(877) 322-8228, or
Write to	Annual Credit Report Request Service PO Box 105281 Atlanta, GA 30348-5281

Security at Fifth Third

Fifth Third Bank values your business and the trust you have placed in us. We take the security of your accounts and confidential information very seriously and employ a variety of tools, techniques, and processes to help protect them.

Security Technology

Fifth Third monitors the constantly changing security landscape to identify and evaluate possible threats against Fifth Third's computer systems and employs various technologies to help protect against those possible threats.

- **Encryption**

  All online activity involving transactions or the transfer of confidential customer information is encrypted from the time it leaves your computer until it enters our systems. Encryption is the process of transforming information into an indiscernible coded message. Information transmitted while accessing account information over the Internet or submitting an online application is encrypted using Secure Sockets Layer (SSL) Technology, a state-of-the-art encryption process developed by Netscape Communications Corporation, which prevents data from being read, if intercepted during transmission.

  This process utilizes a unique mathematical formula or "key" to encrypt your information. Encryption strength is measured by the length of the "key" used to encrypt the data. Longer "keys" provide more effective encryption. Browsers generally offer two levels of encryption strength:

  – 40-Bit Encryption Key (International Grade Encryption) measures 2^{40} possible keys.
  – 128-Bit Encryption Key (Domestic Grade Encryption) measures 2^{128} possible keys.

  When using the Internet, look for the letter "s" at the end of "https" at the beginning of the URL address (e.g., "https://direct.53.com") before entering any confidential information. The "s" indicates that the site is secure.

- **Digital Certificate**

  A Digital ID is an electronic fingerprint bonded to the "keys" used to encrypt information transmitted over the Internet. Referred to as a Digital Certificate, the unique identifier substantiates Fifth Third Bank's identity to your browser.

  Fifth Third Bank is registered with the certificate authority, VeriSign, and has obtained digital certificates for www.53.com and its sub-domains. To check the validity of the site's certificate and authenticity, please click the VeriSign seal.

  VeriSign Secured
  VERIFY

- **Authentication**

  With the growing use of online banking, it is important for us to continue providing additional layers of protection to ensure the security of your transactions. Three security layers include:

  - **User IDs and Passwords** provide the first line of security to protect your information. Password distribution is controlled systematically with the initial temporary password sent to the user's email address designated by the client's System Administrator. Initial passwords are temporary and must be changed upon first use. Users are required to change their password every 30 days.
  - **Risk-Based Authentication** monitors login risks and prompts a user with their pre-defined identification questions in cases where the login risk is above a certain threshold. Risk-based authentication watches for uncharacteristic or unusual login behavior such as logging in from a new location, a different time zone, different Internet Service Provider, etc. If anything "out of the ordinary" is detected, you may be prompted to answer identification questions. This helps us ensure that it is you who is accessing your account.
  - **Go ID** is our token-based authentication required for all users with payments capabilities (e.g., ACH or Wire Transfers). When logging into your account, you will be prompted to enter a six-digit code provided on your Go ID token along with your user ID and password. This additional level of security will help to strengthen your online banking experience.

Token Management - Best Practices

Managing the security of your token device is important to maintaining a secure banking environment. The following are best practice recommendations.

- Place your token in a securely locked environment (desk drawer, file cabinet, etc…) when not in use
- When traveling, keep your token device with you or locked in your hotel room safe
- Do not store your User ID, Password, and token device together
- Never give your token device to another person
- Never give your token's security value to another person for any reason

Online Payments Administrative Controls

It is important to implement controls to prevent unauthorized payment initiation by unauthorized employees or criminals. Fifth Third Bank's Account Management & Payments (AMP) has several levels of permission type settings that allow you to control, monitor and mitigate overall risk exposure.

- **Access to View Accounts:** Managing access to accounts is the first step towards mitigating the risk of potential loss. Fifth Third Account Management & Payments (AMP) allows your organization to manage access to accounts across your organization or at the user level. Account Management & Payments (AMP) allows larger organizations to create distinct units to further control access to information and payments, which may include operating divisions, departments, and teams.

– **Permissions**: Permissions can be managed at four different levels – company, division, group and user. Most permissions are categorized at a company or individual level. Company permissions refer to permissions that apply to the entire company. Per Account permissions allow you to set permissions uniquely for one account.

– **Dollar Limits:** You are encouraged to leverage dollar limits when establishing payment origination permissions for ACH, Account Transfer and Wire Transfer. Some of the dollar limit restrictions available include:
  - Account Transfer per transaction and/or per day limits
  - ACH per batch credit, daily credit, per batch debit and daily debit limits
  - Wire Transfer per transaction and/or per day limits
  - The ability to exceed established dollar limits with secondary approval

– **Payments & Transfers**: Additional payment restrictions are available in addition to dollar limits. You have the ability to assign access to payment types and options at broad or detailed levels for each user and across your broader company. Some of the payments restrictions available include:
  - ACH payment entry, ACH template creation and/or maintenance, ACH type (CCD, PPD, etc.), ACH approval and Participant management
  - Wire payment type (domestic, US denominated, etc.), Wire function (template, freeform), Wire approval (template, freeform), and Beneficiary management

– **Payment Approvals**: Establishing payment approvals is one key method of managing payment risk. You can set up an Approval Workflow to determine eligible approvers for payments that require approval. Permissions, established by your company, determine if a payment requires an approval and the workflow determines who can approve, based on the dollar amount and users in the workflow. The workflow is flexible and can do the following:
  - Establish one or multiple dollar thresholds; each with distinct approval rules
  - Establish rules and thresholds for each type of payment

– **Reporting**: Monitoring payment activity is essential to managing payment initiation. Audit reports provide access to changes in user permissions and system activity. The reports provide the ability to verify user entitlements and dollar limits and to view system activity across all users and across the entire company.

Secure Communications

In addition to securing our systems and the information that flows into and out of them, Fifth Third understands the need to communicate with our clients in a secure manner. Fifth Third will NEVER send you an email asking you to click a link to verify or supply personal information, such as:

- User IDs
- Passwords
- Social Security Number
- Card or Account Numbers
- Credit Card Security Code (CVV)

- Mother's maiden name or other user-defined challenge information (e.g., place of birth, etc.)

If you are unsure about an email or a Website that appears to be from Fifth Third, take the following precautions:

- Type our Website address (www.53.com) into your browser to visit our Website instead of relying on links in emails or an entry in your Favorites.
- Double click on the lock at the bottom of the page to verify that the security certificate is listed as being issued to "www.53.com." Fifth Third is committed to providing a secure online banking experience. Our Website is certified by the VeriSign Secure Site Program.

Glossary

Administrator Profile/Privileges
A computer profile that enables the user to do anything on a computer. Most users do not need and therefore should not have this level of access. Common capabilities included with administrator privileges are the ability to download and install software and to change security settings.

Adware
Software that automatically plays, displays, or downloads advertising material to a computer. It is usually integrated into or bundled with a legitimate program as a way to recover programming development costs, and in some cases it may allow the legitimate program to be provided to the user free of charge or at a reduced price.

Anti-Spyware
Software that identifies and disables software designed to look for and collect information about the user without the user's consent.

Anti-Virus
Software that identifies and disables or quarantines computer viruses and worms.

Backdoor
A backdoor in a computer system is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

Crimeware
Another term for Malware.

Cookies
Pieces of information generated by a Web server and stored on the user's computer. Cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences and the contents of their electronic shopping carts.

Domain
A machine or virtual host on the Internet.

Encryption
The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Firewall
An integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system and to monitor transfers of information to and from a network or computer.

Fraudster
A criminal who tricks victims into exposing themselves to fraud.

Fraudulent Website

A Website that replicates another Website for the purposes of tricking victims into believing it is the legitimate Website and revealing sensitive information. The collected information is then used for illegal activities.

Hacker

A person who enjoys exploring the details of programmable systems and how to stretch their capabilities or identify new ways of doing things. This term has more popularly come to describe a subset of hackers, malicious meddlers who try to discover sensitive information or ways around computer security systems.

Identity Theft

The crime of obtaining the personal or financial information of another person for the purpose of assuming that person's name to make transactions or purchases.

Intrusion Detection

An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and Malware (viruses, trojan horses, and worms).

Key Logger

Dangerous software or hardware that records a user’s keystrokes and makes the collected information available to a third party.

Login Credentials

A person’s user ID or username and password or PIN.

Malware

Malicious software, such as viruses, intended to damage or disable a computer system or steal information without the computer user’s informed consent or knowledge.

Phishing

Phishing occurs when someone impersonates a legitimate company or organization using email, faxes, and Websites in an attempt to entice recipients into revealing confidential information. The phishers’ emails, Websites, and other methods of communication are usually very difficult to distinguish from those of the companies they impersonate.

Risk-Based Authentication

Monitors login risks and prompts the user with their pre-defined identification questions in cases where the login risk is above a certain threshold.

Rootkits

A software system that consists of a program, or combination of several programs, designed to hide or obscure the fact that a system has been compromised. An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker has installed, along with the presence of the rootkit.

SMiShing

A form of criminal activity using social engineering techniques similar to phishing. The name is derived from "SMs phISHING". SMS (Short Message Service) is the technology used for text messages on cell phones. Similar to phishing, smishing uses cell phone text messages to deliver the "bait" to get you to divulge your personal information. The "hook" (the method used to actually "capture" your information) in the text message may be a web site URL, however it has become more common to see a phone number that connects to an automated voice response system.

Social Engineering

Techniques used to trick people into revealing passwords or other information that compromises a computer system, person or company. Classic scams include calling a person who has the required information and posing as a field service technician or a fellow employee with an urgent access problem. Although social engineering is used by many people in the course of their everyday work, “social engineering” in this document refers to actions taken by people to gain access to information or computing resources that are then used for malicious purposes.

Social Networking Sites

Websites used to connect with people who share personal or professional interests, place of origin, education at a particular school, etc. Some examples include Facebook, MySpace, and LinkedIn.

Spyware

These programs range in capabilities and may record some or all of the following information: keystrokes, emails, chat room conversations, instant messages, Websites visited, programs run, time spent on Websites, user names and passwords. Unbeknownst to the victim, these programs transmit the collected or tracked information to or store it for remote retrieval by a third party.

Strong Password

Passwords that are difficult for anyone other than the computer user to guess either by using inside knowledge of the user or automated password “cracking” tools. Strong passwords generally contain a mix of numbers, symbols and upper- and lower-case letters; do not contain any words that can be looked up in a dictionary or common number-letter substitutions; and have as many characters as possible.

System Monitors

Software that tracks the activity of a computer or computer system. Key loggers are a common example of system monitors.

Trojan or Trojan Horse Software

Malicious code that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. Unlike some other forms of Malware, like viruses and worms, trojans cannot operate autonomously. Trojans rely on the intended victim taking certain action to install and activate the programs.

Virus (Computer)

Software capable of causing great harm to files or other programs on a computer. Viruses cannot spread from computer to computer on their own; they usually access new victims through infected email attachments. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

Vulnerability Management

The identification and management of weaknesses in a computer system to minimize the risk of the system being compromised or harmed.

Vishing

Vishing is the practice of using telephone technology to obtain personal and financial information from people for the purpose of financial reward. The term is a combination of "voice" and “phishing”.

Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations that are known to the telephone company, and associated with a bill-payer. However, with the advent of VoIP, telephone services may now terminate in computers, which are far more susceptible to fraudulent attacks than traditional "dumb" telephony endpoints.

Worm

A self-replicating computer program that uses a computer network or email to send copies of itself to other computers without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

References

Anti-Phishing Working Group. *Phishing Activity Trend Report: First Quarter 2008,* www.APWG.org. The Anti-Phishing Working Group, August 2008.

Anti-Phishing Working Group. *Phishing Activity Trend Report: Second Quarter 2008,* www.APWG.org. The Anti-Phishing Working Group, December 2008.

Anti-Phishing Working Group. *Phishing Activity Trend Report: Second Half 2008,* www.APWG.org. The Anti-Phishing Working Group, March 2009.

Brain, Marshall. *How Computer Viruses Work*, www.computer.howstuffworks.com/virus5.htm.

Coursen, Shane. *Viruses: Not Just For Kids Anymore – Protecting Against Attacks,* Computer Security Institute's 33rd Annual Computer Security Conference & Exhibition. Kaspersky Lab, November 7, 2006.

Emigh, Aaron*. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, A Joint Report of the US Department of Homeland Security, SRI International Identity Theft Technology Council, and the Anti-Phishing Working Group.* The US Department of Homeland Security, SRI International Identity Theft Technology Council, and the Anti-Phishing Working Group, October 2006.

Eschelbeck, Gerhard. *The State of Spyware,* Computer Security Institute's 33rd Annual Computer Security Conference & Exhibition. Webroot Software, Inc. November 7, 2006.

Kerstein, Paul. *How Can We Stop Phishing and Pharming Scams?,* www.csoonline.com. July 19, 2005

Kirk, Jeremy. *Phishing Scam Takes Aim at MySpace.com*, IDG Network. June 02, 2006.

McAfee, Inc. *2009 Threat Predictions*. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf.

McGlasson, Linda. *Identity Theft Victims Assistance – Helping Financial Institutions and Their Customers Fight Back Against ID Thieves.* www.BankInfoSecurity.com. December 14, 2007.

McGlasson, Linda. *Phishing Season; Fraudsters Step Up Attacks on Financial Institutions.* www.BankInfoSecurity.com. April 28, 2008.

Microsoft Corporation. *Don't Let Your Company Get Hooked by Phishing*, http://www.microsoft.com/. Microsoft Corporation, July 27, 2005.

Microsoft Corporation. *Microsoft Phishing Filter: A New Approach to Building Trust in E-Commerce Content*, http://www.zdnet.com/. Microsoft Corporation, November 2006.

Moscaritolo, Angela. *Phishing Increased 40 Percent In 2008.* www.scmagazineus.com. April 15, 2009.

Rogers, Jack. *Gartner: $3.2 Billion Lost To Phishing Attacks In One Year.* www.scmagazineus.com. December 18, 2007.

Sophos Plc. *Spyware – the hidden threat to business security*, www.sophos.com. Sophos Plc, July 2006.

Stallman, Richard. *On Hacking*, http://www.stallman.org/.

Symantec Corporation. *Symantec Internet Security Threat Report: Trends for January 06-June 06, volume X*, www.symantec.com. Symantec Corporation, September 25, 2006.

Symantec Corporation. *What You Need to Know About Phishing*, www.clubsymantec.com. Symantec Corporation.

Tom Jagatic, Nathan Johnson, Markus Jakobsson, and Filippo Menczer*. Social Phishing*. Communications of the ACM. School of Informatics, Indiana University; December 12, 2005.

Webroot Software. *From Viruses to Spyware: In the Malware Trenches with Small and Medium-Sized Businesses,* www.Bnet.com. Webroot Software, Inc.

Wikipedia.com entries for the following terms:

- Adware
- Backdoor
- Botnet
- Computer virus
- Encryption
- Hacker
- HTTP cookie
- Keystroke logging
- Malware
- Phishing
- Rootkit
- SMiShing
- Social engineering
- Trojan horse (computing)

Additional Resources

Identity Theft

http://www.idtheftcenter.org/. The Identity Theft Resource Center (ITRC) is a nonprofit program dedicated to providing consumer and victim support and advising governmental agencies, legislators, and companies about this evolving and growing crime.

www.ftc.gov/bcp/edu/microsites/idtheft//. This Website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

Phishing

www.APWG.org or http://www.antiphishing.org/. The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing.

www.wikipedia.org/wiki/Phishing. This Website explains some common phishing methods and dangers.

Security Awareness

www.sans.org/reading_room/whitepapers/awareness/. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The documents at this site will give you ideas on how to heighten security awareness in your organization.

Security Best Practices

www.cert.org/archive/pdf/secureit_bestpractices.pdf. This document presents an approach for evaluating and selecting information security best practices for your organization.

Spyware

www.wikipedia.org/wiki/Spyware. A very detailed look at what spyware is, how it attaches itself to computers, and the common methods of prevention.