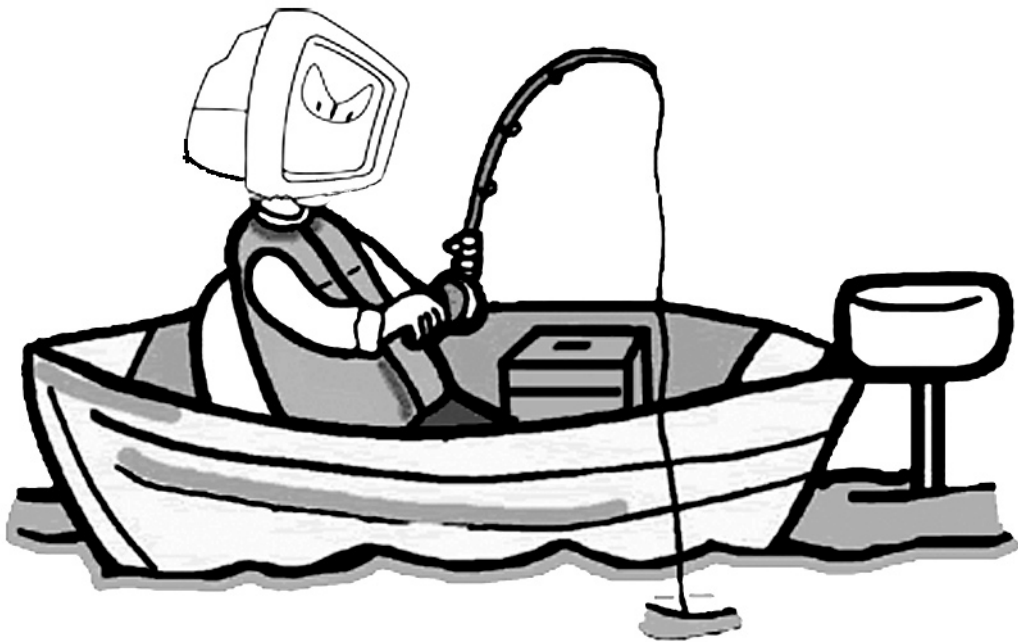


# PHISHING FOR SUCKERS



## HOW TO AVOID GETTING HOOKED

---

By Ed Collins

The e-mail that Phil Roberts received that morning on the Internet seem legitimate. It even had his bank's logo in the message box and appeared signed by the bank's vice president.

But the message itself was disturbing to Phil. The bank said they noticed unusual activity in his account and asked him to verify some sensitive personal data, such as his bank PIN (personal identification number), and account numbers for both his checking and savings accounts.

Naively, Phil responded without giving the request much thought simply by using the convenient return link in the e-mail.

It was only a few hours later that a real official from his bank was on the phone to him reporting that indeed there were some unusual electronic withdrawals taking place in his name. Both his checking and ample savings accounts were suddenly well overdrawn.

Thus began a long nightmare for Phil in attempting to put his financial affairs back in order. He realized to his dismay that he had been hooked by a "phisher."

Phishing, and its second cousin identity theft, are the two fastest growing internet security threats in the nation. Over the past five years more than 27 million people have had their identities stolen. That's about one out of every ten people living in the United States.

First Data Corp. one of the nation's largest electronic financial transaction companies, conducted a survey recently which showed 43 percent of all adults have received a phishing contact, and five percent of them provided personal information which could be used against them.

Phishing scammers cost the nation's banks and credit card issuers well over \$2 billion last year, and costs continue to mount.

Recent security breaches include the loss of 4 million CitiFinancial account files while computer records were being transferred. Another report from Motorola indicated that two computers containing sensitive employee financial information was stolen over a long holiday weekend causing concerns over identity theft.

A virus attack captured customer data from a credit card processing card company jeopardizing the identities and transactions of millions of credit card holders from some of the nation's leading credit card companies.

And here in the Chicago area a local bank serving the communities of North Aurora, Geneva, Batavia and St. Charles issued a phishing warning on its web site after a group of public employees from a local school and a park district received e-mails from a bank imposter asking for verification of account numbers and other sensitive information. Fortunately, none were provided.

The bank president made it clear on their web site, and by other means, that it is bank policy to never contact its customer base by e-mail to verify account information.

### What's phishing?

The U.S. Department of Justice, Criminal Division, defines "phishing" as a general term for the creation and criminal use of e-mails and web sites for fraudulent purposes.

These e-mails and web sites are usually cleverly disguised to

appear as legitimate businesses, such as banks, financial institutions or governmental agencies. Indeed, they often copy logos and company data from legitimate business web sites and modify it for their criminal purposes.

They are purposely created to deceive Internet users into disclosing confidential personal or financial data, passwords, account numbers, etc.

Phishing e-mails often include false reports or startling statements designed to create the impression that there is an immediate threat or risk to your credit card standing or bank account, such as someone else is using your card or account. The intent is to get you to immediately respond.

Promising a "prize" or other incentive to dupe you into responding is another gimmick frequently used by phishers.

Since these crooks make very plausible personal pitches but are forced to use mass e-mailing spamming techniques, only a very small segment of the phony e-mail will match the interest of a particular user. But that's what phishers strive for - to make a match. All they seek is your mouse click in their response box and you will be hooked into one of the biggest nightmares you've ever faced.



---

**Promising a "prize" or other incentive to dupe you into responding is another gimmick frequently used by phishers.**

---

### Three good rules

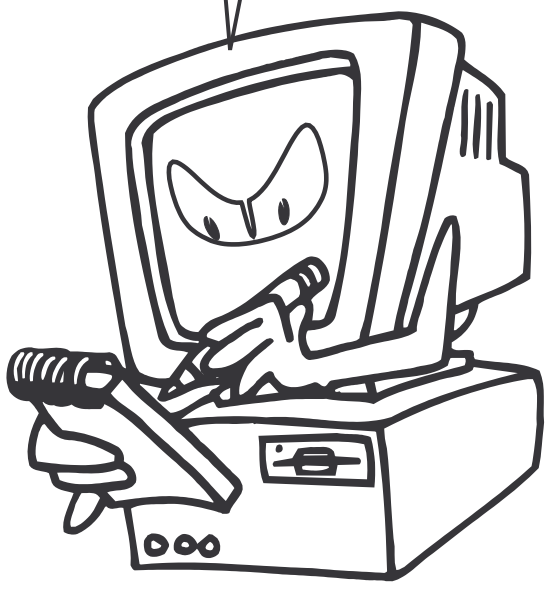
What can computer users do to protect themselves? The U.S. Department of Justice recommends three simple rules when you receive an e-mail, or a possible web site which looks suspicious: Stop, look and call!

**Stop:** Phishers typically include some upsetting, or exciting but false, information to get you to react immediately by clicking on the "handy link" they supply to catch you while off guard. You must resist that immediate impulse to click. There's always enough time to protect yourself by checking and verifying the information carefully.

The Federal Trade Commission says that e-mailing financial and personal details is never a good idea. Most companies don't ask for this over the Internet.

Continued on page 10

And you PIN is ?



They realize that even so-called "secure" lines can have their problems.

Look: You need to look at, and analyze very closely, the claims being made in the e-mail. Do they make sense? Be extremely suspicious of e-mail requests for personal information such as bank or Social Security account numbers, passwords, PIN (personal identification) numbers and other confidential information. No legitimate company asks for this type of information over the Internet.

Think about it - why would a bank be asking you for, or to confirm, an account number. They should already have it! They assigned the number to you in the first place.

Beware also of winning a so-called "prize." Ask yourself why they would be giving you such a prize. Do you recall applying for one? Be cynical. Remember, there's no free lunch! There are always strings attached.

Call: If an e-mail purports to be from a legitimate financial institution or business, pick up your telephone and ask the person (or the manager if there is no name) if they really did send such an e-mail (but don't call phone numbers which were included in the phony e-mail).

Credit card companies usually include toll-free numbers on the backs of their cards, and bank phone numbers are usually listed in the local telephone book, or on their monthly bank statement.

Possible phishing schemes should be promptly reported to law enforcement officials.

If you receive an e-mail with the telltale phishing characteristics, do NOT respond back. Instead, forward the suspicious e-mail to the Federal Trade Commission at [uce@ftc.gov] and copy the AntiPhishing Working Group, a law enforcement oversight agency, at [reportphishing@antiphishing.org]

If you have already disclosed personal information to a possible phisher, you should notify your banks and credit cards to freeze accounts, and immediately file an online complaint with the Internet Crime Complaint Center at [http://www.ic3.gov]

This agency is a joint project of the FBI and the National White Collar Crime Center.

Sucker



Mail Theft  
http://www.usps.com/postalinspectors/id\_intro.htm

**Even in today's world of fast-evolving technologies, U.S. Mail remains one of the most secure means of transmitting personal information.**

Here are some things you should know about identity theft:

- FTC research indicates that you are three times more likely to suffer the theft of financial information via the phone or the Internet than by the U.S. Mail.
- Postal Inspectors take full advantage of the "paper trail" of the mail to help prevent and combat identity theft.
- The U.S. Postal Service delivers more than 206 billion pieces of mail a year to roughly 142 million customers at some of the most affordable postal rates in the world. U.S. Postal Inspectors are mandated to safeguard all of it "including the people who move it and the customers who use it" and it's all included in the price of a stamp.

For more information, read our brochure, Publication 280, [Identity Theft](#).

[Inspection Service Home](#)

[www.usps.com/postalinspectors/id\\_intro.htm](http://www.usps.com/postalinspectors/id_intro.htm)

How Not to Get Hooked by a 'Phishing' Scam  
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingart.htm

FEDERAL TRADE COMMISSION  
FOR THE CONSUMER

HOME | CONSUMERS | BUSINESSES | NEWSROOM | FORMAL | ANTITRUST | CONGRESSIONAL | ECONOMIC | LEGAL  
Privacy Policy | About FTC | Commissioners | File a Complaint | HSR | FOIA | IG Office | En Español

FTC Consumer Alert

How Not to Get Hooked by a 'Phishing' Scam

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing"—and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, phishers send an email or pop-up

<http://www.ftc.gov/bcp/conline/pubs/alerts/phishingart.htm>

## Suggested Internet reading

Phishing: How Not to Get Hooked by a Phishing Scam, Text developed by the Federal Trade Commission. Use web page: <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingart.htm>

Identity Theft. Visit the Dept. of Justice's web pages at: <http://www.usdoj.gov/criminal/fraud/idtheft.html>  
<http://www.usdoj.gov/criminal/fraud/idquizz.html>

Identity Theft, Postal Inspectors Service, use web page: [www.usps.com/postalinspectors/id\\_intro.htm](http://www.usps.com/postalinspectors/id_intro.htm)

Cybercrime, Visit Dept. of Justice's web site at: <http://www.cybercrime.gov>

Identity Theft: A Quiz for Consumers  
http://www.usdoj.gov/criminal/fraud/idquizz.html

Criminal Division  
Department of Justice

Identity Theft: A Quiz for Consumers

Identity thieves use many ways of getting your personal financial information withdrawals from your accounts. Do you know how you can reduce the risk of this quiz, and see how you score:

	Yes	No
1. <b>When I keep my ATM cards and credit cards in my wallet, I never write my PIN (Personal Identification Number) on any of my cards.</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reason: If you lose your ATM or credit card, identity thieves or other criminals can have instant access to your bank or credit-card account.		
2. <b>When I leave my house, I take with me only the ATM and credit cards I need for personal or business purchases.</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reason: If your wallet or purse is lost or stolen, and you're carrying fewer cards, you'll have to make fewer calls to banks and credit-card companies to report the losses, and the odds of fraudulent charges in your name will be lower.		
3. <b>When I get my monthly credit-card bills, I always look carefully at the specific transactions charged to my account before I pay the bill.</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reason: Someone who gets your credit-card number and expiration date doesn't need the actual card to charge purchases to your account. If you don't look closely at your credit-card statement each month, you might not have any recourse if fraudulent transactions go through and you don't		

<http://www.usdoj.gov/criminal/fraud/idquizz.html>

## Nuisance calls can be cut by using Do Not Call Registry

Tired of receiving unwanted telemarketing calls? Then register your home or cellular phone on the Federal Trade Commission's national Do Not Call Registry.

While the registry will not eliminate all such unwanted calls, it will reduce many of them.

To register over the Internet go to [www.donotcall.gov](http://www.donotcall.gov) and follow the instruction provided. After a few simple questions such as what phone number you would like to register (you are allowed up to three), and a valid e-mail address that the FTC can use for your confirmation, you will be on the registry.

You will receive an e-mail confirming your request. You must reply within 72 hours to activate.

You can also register by phone calling 1-888-382-1222. Just follow the instructions to enter your phone number (you can only register the number you are calling from).

Don't expect these nuisance calls to stop immediately. Usually they will after a one to three month period. Some companies will still be allowed to call, such as political organizations, charities, and companies with whom you have an established past business relationship.

Both the Federal Trade Commission, and the Illinois Attorney General's Office, are charged with enforcement. Violators, if identified, can be fined up to \$11,000 per violation.