

A decorative graphic consisting of two overlapping, curved shapes resembling folded paper or a ribbon. The top shape is yellow and the bottom shape is blue, both pointing towards the right.

# Cut the Line on Phishing Scams



Fraudsters looking to gather financial information have developed a new way to lure unsuspecting victims: they go phishing.

## “PHISHING FOR INFORMATION”

Phishing, also called “brand spoofing” is the creation of e-mail messages and Web pages that are replicas of existing, legitimate websites and businesses for the purpose of committing fraud. These Web sites and e-mails are used to trick Internet users into sending personal, financial, or password data. Phishing e-mails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud.

The word phishing comes from the analogy that Internet scammers are using e-mail as lures to ‘fish’ for passwords and financial data from the sea of Internet users.

It is important to know that neither Visa nor its Member financial institutions solicit personal information via e-mail. If you receive an e-mail appearing to be from Visa, contact Visa immediately at: [phishing@visa.com](mailto:phishing@visa.com). To report possible phishing scams from other organizations, send an e-mail to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org).

## **What is phishing?**

Phishing is the act of sending an unsolicited e-mail to an Internet user falsely claiming to be a legitimate enterprise in an attempt to scam the Internet user into disclosing private information. These e-mails often ask the Internet user for personal information such as credit card numbers, bank account information, social insurance numbers, and passwords. The goal of criminals using brand spoofing is to lead consumers to believe that a request for information is coming from a legitimate company - usually one they do business with. In reality, it is a malicious attempt to collect customer information for the purpose of committing fraud.

## **How does phishing work?**

Customers are sent an unsolicited e-mail appearing to be from a legitimate company that the customer deals with - for example their Internet Service Provider (ISP), online payment service, or financial institution. The e-mail claims that a billing error or account problem has occurred, or that the consumer's information needs to be updated or validated. Customers are then asked to follow instructions that will take them to a Web site that appears legitimate, complete with a company's brand name, corporate logo, and corporate colours - otherwise known as a "brand spoofed" Web site. While at the site, customers are asked to update personal and financial information by completing an online form. The form requests a variety of information such as credit card numbers, account numbers, passwords, date of birth, driver's license number, and social insurance numbers.

Because these Web sites and e-mails often look authentic and "official", some recipients are fooled into responding, and thereby disclosing their financial and personal information to criminals. These criminals then use the information to purchase goods and services, obtain credit, or commit identity theft.



## Reporting a phishing e-mail to Visa

If you've received what you suspect to be a phishing e-mail appearing to be from Visa, please report it by sending an e-mail to [phishing@visa.com](mailto:phishing@visa.com), by following these simple steps:

### Assuming you use Outlook or Netscape:

1. Create a new mail message to [phishing@visa.com](mailto:phishing@visa.com).
2. Drag and drop the phishing e-mail from your inbox onto this new e-mail message. In Netscape drop it on the 'attachment' area.
3. Do not use the "forward" function because it loses information and this requires more manual processing. The exception to this is when you use the Web interface to Outlook, in this case forwarding the message is the only option.

To report phishing scams from other organizations, send an e-mail to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org), and follow the steps listed above.

## Tips on how to spot and avoid phishing and "brand spoofing" scams:

- **Protect your computer.** You can protect your computer, your sensitive files, and your home network from hackers and viruses by taking some basic precautions. Use tools to fight back and protect your computer and your information. Some easy-to-use tools are **anti-virus software, spyware filters, e-mail filters, and firewall programs** [for high-speed (broadband) connections].

**Anti-virus software** scans your computer and your incoming e-mail for viruses, and then deletes the viruses. To make sure your software offers the highest level of protection, you must update your anti-virus software regularly. Most commercial anti-virus software include a feature which allows you to download updates automatically when you are on the Internet.



Many of the current anti-virus programs on the market also provide anti-spyware programs. Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. It is a good idea, when obtaining anti-virus software, to select one that also has **anti-spyware** capability.

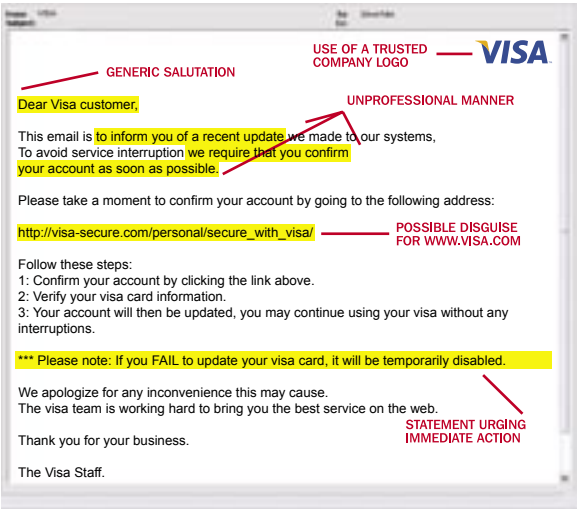
Most e-mail providers have **e-mail filters** built-in to the application. These filters block out unwanted e-mail such as spam.

Broadband users should take extra precautions to secure their computer and their computer files. The speed at which information can be transferred to and from your computer, and the fact that it stays connected to the Internet for long periods of time, makes it a target for hackers. A **firewall** is a software program or piece of hardware that prevents unauthorized Internet traffic from entering or leaving your computer. The best way to ensure protection is to use both a firewall and anti-virus software.

- **Be alert for scam e-mails.** If you get an unsolicited e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, **do not** reply or click on the link in the e-mail.

Phishers typically include upsetting or exciting (but false) statements in their e-mails to get people to react immediately. These e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are.

## Below is a sample of a typical phishing e-mail:



If you've received one of these suspicious e-mails, report it to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org); or if the e-mail appears to be from Visa, report it to [phishing@visa.com](mailto:phishing@visa.com). Do not click on any links provided in the e-mail, as this may introduce a Trojan program into your network or computer.

## WHAT IS A TROJAN PROGRAM?

Trojan programs install themselves into your computer without your knowledge, and can track the keystrokes you make, thereby giving criminals access to your personal information.

- **Contact Visa or your financial institution immediately and report your suspicions.** If you receive an unsolicited e-mail that you are suspicious of and that appears to have been sent by a Visa financial institution, or by Visa itself, contact your financial institution, or Visa at [phishing@visa.com](mailto:phishing@visa.com). To report possible phishing scams from other organizations, send an e-mail to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org).



- **Do not reply to any unsolicited e-mail that requests your personal information.** Do not respond to unsolicited e-mails that ask for sensitive financial information such as your credit card number, the last three digits printed on the signature panel on the back of your credit card, bank account number, driver's license number, or social insurance number. Also be wary of any e-mail that sends you personal information about yourself and asks you to update or confirm it.
- **Be aware when submitting personal or financial information on Web sites.** Before submitting financial information through a Web site, look for the "padlock" icon on your browser's status bar – this signals that your information is secure during transactions.
- **Be aware.** Phoney "look alike" Web sites are designed to trick consumers into giving out personal information, which is then collected and used in fraudulent activities. Make sure that Web sites on which you do business post privacy and security statements. You should review these carefully. Always ensure that you're using a secure Web site when submitting credit card or other sensitive information. To make sure you are on a secure Web server, check the beginning of the Web address in your browser's address bar – **it should read "https://"**, rather than "http://".
- **Look for misspelled words.** Misspelled words either in the message, hyperlink or Web site often signal "phishing" scams.
- **Be careful before clicking on a link contained in an e-mail message.** If a link is provided in the message, do not click on it because it may take you to a fraudulent Web site. If you click on a link in the e-mail, you may introduce a Trojan program into your network or computer. Instead, type the company's Web address in the address bar of your browser. If you don't know the address, use a search engine and search for the company's name to help you locate it. Once on the site, search for any information, bulletins or notices that convey the same message provided in the e-mail you received.

- **Leave suspicious sites.** If you suspect that a Web site is not what it claims to be, leave the site immediately. Do not follow any of the instructions it provides.
- **Monitor your transactions.** Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balance. In addition, you should also regularly log into your online accounts.
- **Always report phishing or “spoofed” e-mails.** If you receive a suspicious e-mail appearing to be from Visa, contact Visa immediately at: [phishing@visa.com](mailto:phishing@visa.com). To report possible phishing scams from other organizations, send an e-mail to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org). If you suspect that fraudulent activity has resulted from a phishing e-mail, contact your financial institution and your local police immediately.

## Frequently Asked Questions

### How do I know if I’m being phished?

Be very suspicious of any unsolicited e-mails that urgently request personal or financial information. Most phishing e-mails are not personalized, suggesting the use of a mass e-mail list. Also look for grammatical errors and spelling mistakes.

### What should I do if I suspect that I’ve received a phishing e-mail?

If you receive a suspicious unsolicited e-mail that appears to have been sent by Visa, contact Visa immediately at [phishing@visa.com](mailto:phishing@visa.com). If you believe you’ve been a victim of phishing, contact your local police.

### **How can I ensure that I am communicating with a financial institution during a secure session?**

You can verify that you are communicating with a genuine financial institution by examining the Web site certificate during a secure session. The Web site certificate will verify the identity of the specific Web site you are accessing as well as validate that the site is secure and genuine. It also ensures that no other Web site can assume the identity of the original secure site. Please refer to your Web browser's documentation for instructions on how to view a certificate. Always ensure that you're using a secure Web site when submitting credit card or other sensitive information. To make sure you are on a secure Web server, check the beginning of the Web address in your browser's address bar - **it should read "https://"**, rather than "http://".

### **What should I do if I've already provided my credit or debit card information to a possible phishing e-mail?**

Report the theft of information to the card issuer as quickly as possible. If your *Visa* card was compromised, contact the financial institution that issued your card, **and** send an e-mail to [phishing@visa.com](mailto:phishing@visa.com).

Once you've contacted all relevant financial institutions, cancel your account, and open a new one. Ensure you review your billing statements carefully after the incident. If they show any unauthorized charges, it is best to contact your card issuer and describe each questionable charge.

### **How is my information transmitted safely over the Internet?**

Web browsers use standard security protocols like Secure Socket Layer (SSL), and Secure Hyper Text Transfer Protocol (S-HTTP) to enable private information to be transmitted safely over the Internet. When you visit a Web site with the SSL protocol, a secure connection is created between your computer and the Web site server you are visiting. Once this connection is established, you can transmit any amount of information to the Web server safely. In contrast, the S-HTTP protocol is designed to transmit individual messages securely.

### **How can I tell if my browser session is secure?**

For most Web browsers such as Microsoft Internet Explorer and Netscape Navigator, a secure, encrypted session will be indicated by a closed padlock or an unbroken key icon that appears in the lower left or right hand corner of the browser window. You may also check the address bar of your browser. If the Web site address starts with "https://" rather than "http://" then the session is secure.

### **What do I do if I've downloaded a virus or Trojan program?**

Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames, passwords, Social Insurance Numbers, etc. In this case, you should:

- Install and/or update anti-virus and personal firewall software;
- Update all virus definitions and run a full scan;
- Change all your online passwords;
- Check your other accounts. The hackers may have helped themselves to many different accounts:
  - Check your online auction accounts, your e-mail ISP, online bank accounts, online trading accounts, e-commerce accounts, and everything else for which you use an online password.

## **What is a Digital Certificate and how does it help to ensure security?**

Digital Certificates are issued by extensively audited and controlled certification authorities to authenticate a Web site or elements of Web sites. The certificate identifies the originator of the site and verifies that it has not been tampered with. When your Web browser is presented with a certificate, it will check to see if a legitimate certification authority issued the certificate. If there is a match, your session will continue. Otherwise, your browser will issue a warning, and your safest action is to cancel your activity.





™ Trademark of Visa International Service Association; Visa Canada Association is a licensed user.