

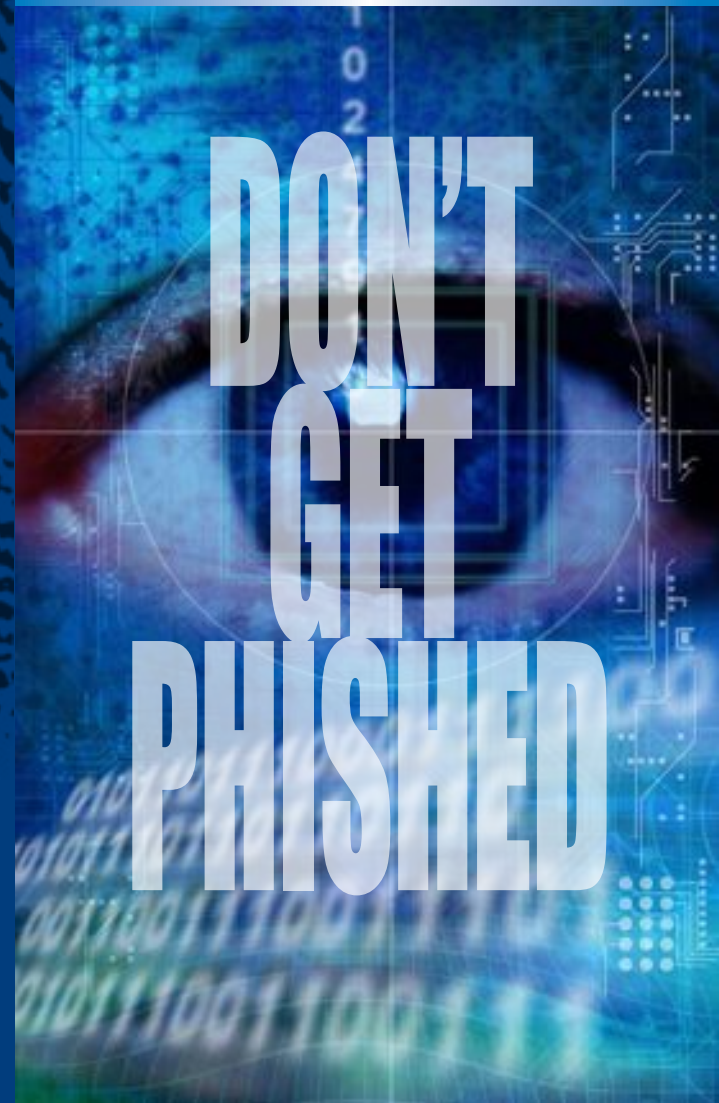


OTHER WAYS TO PROTECT YOUR ONLINE SECURITY (continued)

- Bookmark Web addresses on your Internet browser for sites you visit frequently, and use only that bookmarked address to access the site.
- Periodically order a copy of your credit report from the three major credit reporting bureaus. You are entitled to one free report each year.
Equifax: (800) 685-1111 www.equifax.com
Experian: (888) 397-3742 www.experian.com
TransUnion: (800) 916-8800 www.transunion.com

OTHER SOURCES OF INFORMATION

- The Privacy Rights Clearinghouse:
www.privacyrights.org
- The Federal Trade Commission:
www.consumer.gov/idtheft



ARE YOU A TARGET? HOW TO PROTECT YOURSELF ONLINE

Considering how much we use electronic media today, keeping our computers and data secure is crucial. USD receives about 730,000 e-mails per day, of which only about 280,000 are legitimate. This gives you some idea of how much garbage is out there.



WHAT IS “PHISHING”?

Phishing e-mails are unsolicited e-mails sent to random e-mail addresses, allegedly from a financial service firm (PayPal, a bank or other financial institution, the IRS, etc.). They appear to be legitimate but are actually a scam designed to obtain your personal information in order to defraud you.

By using the names of established firms and fake Web sites, phishers convince recipients to respond with their personal information. The scammers can then withdraw money from accounts or make other unauthorized transactions.

WHAT PHISHING E-MAILS LOOK LIKE

Look for the following “giveaways”:

- Warnings such as “Your account will be closed or suspended unless....” or “your 2006 tax return is subject to an IRS audit; please provide your....” Or they may include “too good to be true” special offers or promises.
- Links to a fraudulent Web site that closely resembles a company’s actual site. They want you to go to the fraudulent Web site and enter personal information.
- Intentional spelling errors which allow them to bypass spam and virus filters.
- Fields asking you to “update information” or “log-on.” They record the data that is entered and can misuse it for financial or identity theft.
- Links or attachments that, if opened, install spyware which records keystrokes and searches for passwords; the information is relayed back to the phisher.

WHAT YOU CAN DO

- Be wary of any unsolicited e-mail that appears to be from a financial services company requesting personal information, particularly one that tries to scare you.
- Immediately delete any e-mails that you suspect are fraudulent. Report them to the Technical Support Center (TSC@sandiego.edu, (619) 260-7900) and avoid opening them.
- If you do open an e-mail that you suspect is a scam, do not click on any links or open any attachments provided.

OTHER WAYS TO PROTECT YOUR ONLINE SECURITY

- Do not provide personal or account information in response to an unsolicited e-mail. Call the company directly using the company’s 800 number that is printed on your account statement.
- Set up online accounts with your financial institutions when possible and monitor them regularly.
- Do not use your USD username and/or password on any other Web sites. Change your password frequently.
- Do not give your password to anyone.
- Update your operating system and anti-virus software regularly.

