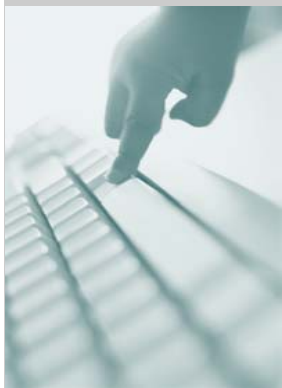


## Phishing Scams

**The damage caused by phishing ranges from loss of access to email to substantial financial loss.**



**Safeguard sensitive and personal information**

It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately \$929 million USD.

Phishing messages are becoming increasingly personalized in attempts to convince the recipients to trust originators of the messages. A phishing email recently submitted to U.S. authorities illustrates this trend. In this case, the message that arrived in the victim's inbox included the person's full name and postal address.

Become CyberAware and protect yourself from Internet scams.



Information Services Department  
Information Security Office  
55 Lake Avenue North  
Worcester, MA 01655

Phone: 508-856-8643—Fax: 508-856-5150  
E-mail: [ITsecurity@umassmed.edu](mailto:ITsecurity@umassmed.edu)  
Web: <http://www.umassmed.edu/IS/ITsecurity>

University of Massachusetts Medical School

## Information Security Awareness Series

### Phishing



**Security Starts with Awareness for Everyone**

# October is National Cyber Security Awareness Month

## Topic of the Week: Phishing

Have you ever been the intended victim of a Phishing scam?



**Protect your identity, and your credit**

“Phishers” attempt to fraudulently gather your personal and financial information by masquerading as a trustworthy person or business in an electronic communication.

Phishing is typically carried out using email or instant messaging, although cell phone contact has been used as well.



## Phishing Techniques


A typical Phishing technique is to convince the user that their account is in jeopardy and request that they follow a web link to ensure that this account remains active. The web link usually involves inputting sensitive information such as account name and number, password, and possibly social security number, and address. Once this data is acquired, the phishers may use a person's information to create fake accounts in a victim's name, ruin a victim's credit, or even prevent victims from accessing their own accounts.

As a secondary attack, the phishing web site sometimes installs spyware on the user's computer. This software could be a keystroke logger or a program which provides the phishers with access to the system.

These scams have their basis in “social engineering” and often involve the phishers posing as a large and trusted entity, such as a big bank or PayPal. We have seen an instance where the phishers posed as the UMass Five College Federal Credit Union! They craft their pages carefully, often using the same web page layouts and logos as the entity they are trying to impersonate.

The best defense to Phishing schemes is to identify phishing attempts before clicking on a web link.

## How to be CyberSafe

- DO NOT OPEN unsolicited email attachments
- USE virus protection software and (auto) update your anti-virus signatures daily
- Protect Personal Information: Make sure that the “Bank’s” website is in fact the original website.  
Clicking on  the lock in your browser will show you the certificate information about the website.
- Beware of Spyware: it is installed on your computer (often without your knowledge or consent) and is used to collect information about you. Spyware usually comes with “free” software that is downloaded from the Internet including screen savers, clip-art, and peer-to-peer clients. Spyware can track which sites you visit, log your keystrokes and send confidential information about you to third parties. Use programs such as Spybot to detect and clean spyware from your computer.



Information Services Department  
Information Security Office

Phone: 508-856-8643—Fax: 508-856-5150

E-mail: [ITsecurity@umassmed.edu](mailto:ITsecurity@umassmed.edu)

Web: <http://www.umassmed.edu/IS/ITsecurity>