

## HOW DO THEY GET MY PERSONAL INFORMATION OR STEAL MY IDENTITY?

Thieves send millions of emails to internet users that ask them to update their account information for banks, credit cards, online payment services or popular shopping sites. Frequently the email claims that the recipient's account information has expired or has been lost and the account holder needs to immediately resend it to the company.

### **SPOOFING (spoo●ing)**

*vi.* An attempt by internet scammers to steal your personal information.



## WHAT IS "SPOOFING"

"Spoofing" (also called "phishing") occurs when thieves send an email that appears to have been sent from the domain of a legitimate retailer, bank, credit card or insurance agency. In recent months, fraudsters have spoofed customers of Citibank, BestBuy, Earthlink, eBay, PayPal and even the Federal Deposit Insurance Corporation (FDIC).

## HOW CAN I TELL IF AN EMAIL IS A SPOOF?

Here are a few things that you should look out for:

### ■ **REQUEST FOR PERSONAL INFORMATION**

Be careful of any email that asks for personal information such as user ID, password or bank account numbers or Social Security Numbers.

### ■ **SENDER'S ADDRESS**

Don't rely on the sender's email address to validate the true origin of the email -- it may look legitimate, but fraudsters can easily alter the "from" field of an e-mail message.

### ■ **GREETING**

Many spoof emails begin with a general greeting such as "Welcome User" rather than a specific, personalized greeting.

### ■ **THREATS TO ACCOUNT**

Many spoofs declare that a recipient's account is in jeopardy and only by authenticating information can an account be kept from being closed, suspended or restricted.

### ■ **LOST INFORMATION**

Consumers should be wary of claims that a company is updating its files or accounts. Legitimate companies with established business practices and strong security measures are not likely to lose account information.

### ■ **LINKS**

Links that look like they connect to a particular site may have been forged. Always open up a new browser window and manually type in the website address.

**THOUGH IT IS DIFFICULT TO DETECT FRAUDULENT EMAILS  
- THERE ARE CERTAIN CHARACTERISTICS INTERNET USERS SHOULD LOOK FOR THAT ARE COMMON TO MANY SPOOF EMAILS**



## AVOID BEING A VICTIM OF SPOOF BY:

Being extremely skeptical of email received from someone you don't know.

Keeping separate passwords for each online account.

Never clicking on a link embedded within any potentially suspicious email.

Calling your financial institutions to verify account status before divulging any information.

Never responding to any request for personal information that comes to you via email.

Updating anti-virus software weekly.

Working from the most current versions of web browsers.

Checking your online accounts regularly.

Installing and running firewalls.

**INDIVIDUALS CAN TAKE SPECIFIC STEPS TO HELP AVOID FALLING PREY TO A SPOOF ATTACK**

## LINKS

**Office of Attorney General, Virginia Computer Crime Unit**

[www.vaag.com](http://www.vaag.com)

email: [cybercrime@oag.state.va.us](mailto:cybercrime@oag.state.va.us)

**Internet Crime Complaint Center**

[www.ic3.gov](http://www.ic3.gov)

*Report phishing emails on this website use the "attempted fraud" category*

**Federal Trade Commission**

[www.ftc.gov](http://www.ftc.gov)

[www.ftc.gov/spam](http://www.ftc.gov/spam)

email: [uce@ftc.gov](mailto:uce@ftc.gov)

**United States Department of Justice**

Special Report on "Phishing"

[www.usdoj.gov/criminal/fraud/phishing.pdf](http://www.usdoj.gov/criminal/fraud/phishing.pdf)

*Contains contact information for legitimate organizations that have been targeted by phishing schemes*

**Anti-Phishing Working Group**

[www.antiphishing.org](http://www.antiphishing.org)

*Includes detailed steps to take if you have disclosed your personal information.*

**Security Centers**

*Many companies also include information on how to stay safe online. You can visit the eBay Security Center, where you can report eBay spoofs, at [www.ebay.com/securitycenter](http://www.ebay.com/securitycenter)*



**Attorney General  
Bob McDonnell**

Commonwealth  
of Virginia



**FOR MORE INFORMATION  
ABOUT PHISHING & SPOOFING  
CONTACT (804)786-2071**

# SPOOFING WEBSITES & EMAILS



**A CONSUMER'S  
SAFETY GUIDE  
TO E-COMMERCE  
FROM THE OFFICE  
OF THE ATTORNEY  
GENERAL,  
COMMONWEALTH  
OF VIRGINIA**

