Microsoft

From: Hotmail Customer Care [MorHezi78@adatum.com] 1
Sent: Thursday, September 18, 2008 8:31 PM
Subject: Verify Your Account now To Avoid It Closed

Windows Live Hotmail

Dear Account User: 2

CONFIRM YOUR WINDOWS LIVE ACCOUNT SERVICES. VERIFY YOUR HOTMAIL ACCOUNT NOW TO AVOID IT CLOSED !! 3

This Email is from Hotmail Customer Care. 4

Due to the congestion in all Hotmail users and removal of all unused Hotmail Accounts, Hotmail would shut down all unused Accounts, You will have to confirm your E-mail by filling out your Login Information below or your account will be suspended within 24 hours for security reasons.

* Username: .....
* Password: .....
* Date of Birth: 5
* Country Or Territory: .....

Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently.

Sincerely,
The Windows Live Hotmail Team

1. A suspicious e-mail address. (Note that the real e-mail address has nothing to do with Windows™ Live® Hotmail.)
2. Generic salutations rather than using your name.
3. Alarmist messages. Criminals try to create a sense of urgency so you'll respond without thinking.
4. Misspellings and grammatical errors.
5. Requests to verify or update your account, stop payment on a charge, or make some other such decision.
6. Amazing offers (not shown). If it sounds too good to be true, it probably is.

Once you get the hang of it, spotting the red flags that characterize a scam isn't hard; you may even find it fun.

Microsoft

More Helpful Info

- The FTC gives thorough advice that can help you deter, detect, and defend against identity theft: **ftc.gov/idtheft**.
- Get more specifics on how to identify and protect yourself from phishing scams: **microsoft.com/protect/yourself/phishing/default.mspx**.
- Visit the Anti-Phishing Working Group for the latest phishing schemes and statistics: **antiphishing.org**.
- Practice your phish-busting skills: **ilookbothways.com/community/learn/spotspam**.

Content contributor LOOKBOTHWAYS The Human Factor in Online Safety

0609 PN 098-115012

Microsoft

Smarter Online = Safer Online

Protecting Yourself From Internet Phishing Scams

Microsoft

What Is a Phishing Scam?

One way to hook a fish is to use a lure so realistic that the fish thinks it's food. Phishing on the Web works the same way. Thieves send an e-mail, instant, or text message or a note through a social networking service (such as MySpace). These pose as a notice from a reputable company right down to the forged sender's address and logo.

The convincing message entices you to divulge sensitive information on the spot. Or it might ask you to call a phony toll-free number or click a link that takes you to a fake Web page. There you're asked to give your Social Security number, an account number, password, or other such info.

Phishers exploit this data themselves or sell it to other criminals. If you take the bait, you could be putting your financial status and your identity at risk.

Spot the warning signs

Your best defense, of course, is caution–and staying alert to the signals of a scam illustrated on the facing page.

Four Ways to Protect Yourself from Phishing

1 Treat suspicious messages cautiously

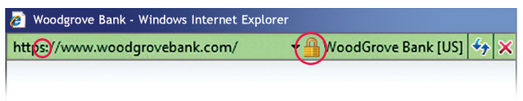
The most dangerous scams are the ones that look genuine. If you get a message in e-mail or on a social site that exhibits some of the warning signs of phishing, here's how to handle it.

- Don't trust the sender, even someone you know or a company you trust. A crook may have hijacked a friend's account and sent e-mail to everyone in that friend's address book.
- Don't respond to the message even to remove your address from the sender's list.
- Don't give sensitive information in e-mail, instant messages, or unexpected pop-up windows.
- Be wary of clicking links or calling the number in the message, even if you think you know the sender; both could be phony.
- Confirm with the sender that the message is real. Call the company's number using a recent statement. Or visit the official Web site by typing the address yourself or using your own bookmark or favorite.

2 Look for signs that a Web page is safe

If you click a suspect link to visit a Web page, before you enter sensitive data check for evidence that:

- The site uses encryption, a security measure that scrambles data as it traverses the Internet. Signs include a Web address with https ("s" stands for secure) and a closed padlock beside it. (The lock might also be in the lower right corner of the window.)



- You're at the correct site–for example, at your bank's Web site, not a counterfeit. If you're using Windows® Internet Explorer®, one sign of trustworthiness is a green address bar like the one shown below left.

If you have even the slightest doubt about the site's legitimacy, play it safe and leave.

3 Reduce spam in your inbox

Share your primary e-mail address and IM name only with people you know or with reputable organizations. Avoid listing them in Internet directories (such as white pages), job-posting sites, and online communities.

Set the spam filters in your e-mail service to Standard or High. In Windows Live Hotmail, for example, click **Options** and then **More Options**; review your options under **Junk e-mail.**

4 Get help from technology

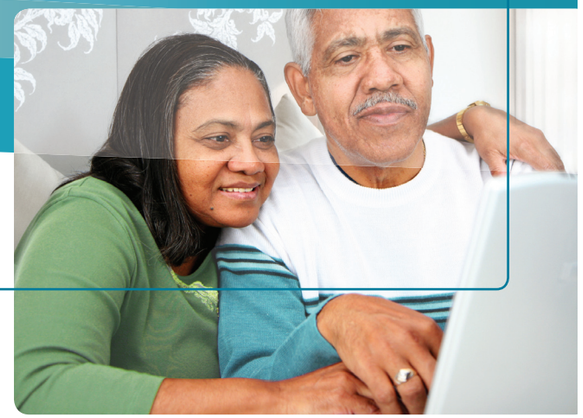
Improve your computer's security. Always use firewall, antivirus, and antispyware software. Keep all software current (including your Web browser) with automatic updates. Password-protect your wireless connection at home. Microsoft can help: **microsoft.com/protect/computer/default.mspx**.

Use a filter that warns you of suspicious Web sites while you surf and blocks visits to reported phishing sites. For example, try the SmartScreen® Filter included in Internet Explorer 8.

Use an e-mail program that builds in anti-phishing detection to help prevent fraudulent e-mail from reaching you. For example, Windows Live Hotmail automatically highlights potentially phishy messages or moves them to the Junk folder.

Microsoft

What to Do If You've Been Hooked by Phishing



Immediately change the passwords and PINs on all your accounts

Immediately report the incident

- If you have given such data as credit card or account numbers, passwords, etc., contact your credit card company or bank. Notify your insurance company if you gave out medical information. They will advise you on next steps such as closing your account or getting new cards.
- If you've been a victim of identity theft, report it to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft** or call toll free: **(877) 438-4338**.

Monitor your account activity

- Continue to check all your credit card and bank statements monthly for unexplained charges or inquiries that you didn't initiate. Regularly log on to any online accounts as a way to make sure no one has changed your password or PIN.
- To help detect potential fraud, request credit reports for yourself and any minor in your care over 14 years of age. Every year, you're entitled to one FREE report from each of the three major U.S. credit bureaus: Experian, Equifax, and TransUnion.

  Consider spacing these requests throughout the year. The easiest way to get them is by visiting **AnnualCreditReport.com** or by calling toll free: **(877) 322-8228**.

If you see something, say something

Report phishing messages even when you haven't been scammed. If nothing else, you may help protect someone from becoming a victim.

Notify the company that's been misrepresented. Look for a special e-mail address to report the scam. For example, if you receive e-mail claiming it's from "Microsoft," forward the message to **abuse@microsoft.com**. Type the e-mail address yourself (rather than relying on one in the message).

Notify the e-mail or social networking service that delivered the scam. Most have buttons for reporting. For example, you can use Internet Explorer 8 for any Web mail. Click the **Safety** button in the upper right corner of the screen. Then point to **SmartScreen Filter** and click **Report Unsafe Website**.

Contact the FTC. Forward the phishing message to **spam@uce.gov**.