## 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 in the same way. Thieves send an email, instant, or text message, or a note through a social network (such as Facebook) or an online game. The message poses as a notice from a reputable organization (like your bank or a favorite charity), so realistic it may include the forged sender's address or logo.

The convincing message entices you to divulge sensitive information. Or it might ask you to call a phony toll-free number or to click a link that goes to a fake webpage. There you're asked to give your Social Security number, an account number, password, or other such information that phishers exploit themselves or sell to other criminals. If you take the bait, you could be putting your credit, money, or identity at risk.

### Spot the warning signs

Your best defense, of course, is caution—and staying alert to the signals of a scam, some of which are shown on the facing page.

## What to do if you've been hooked by phishing

### Immediately change the passwords and PINs on all compromised accounts

Also change them on any accounts where you have used the same password.

### Immediately report the incident

> If you have given data like credit card or account numbers or passwords, contact the financial institution or merchant. Notify your health insurance company if you supplied medical information. They will advise you on next steps such as closing your account, getting a new card, or placing a fraud alert on your credit report.

> If you've been a victim of identity theft, report it to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft**.

### Monitor your account activity

> 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.

> Every year, get your free credit report (and that of any family member over age 14) from each of the major U.S. credit bureaus: Experian, Equifax, and TransUnion. The easiest way to get them is from **AnnualCreditReport.com**.



1011 PN 098-115012

Microsoft

# Protecting Yourself from Phishing Scams

Microsoft

**From:** Hotmail Customer Care [MorHezi78@adatum.com] 1
**Sent:** Thursday, November 10, 2011 8:31 PM
**Subject:** Verify Your Account now To Avoid It Closed

Microsoft 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.

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 fill out your Login Information below or your account will be suspended within 24 hours for security reasons. 4

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

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**

## *Can you spot other examples of these warning signs in this email message?*

1. A suspicious email address. (Note that the real email address is not from 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, and the like.
6. Amazing offers (not shown). If it sounds too good to be true, it probably is.

# Four ways to help protect yourself from phishing

## 1 Treat suspicious messages cautiously

The most dangerous scams are the ones that look genuine. In general, be wary of the sender, even someone you know or a company you trust. A crook may have hijacked a friend's account and sent email to everyone in the friend's address book.

> Don't respond to the message even to remove your address from the sender's list.

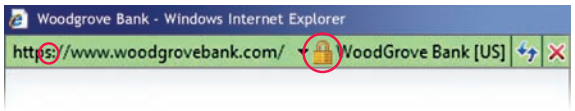
> Don't put sensitive information in an email, instant, or text message, or unexpected pop-up window.

> Think before you click links or call a number in the message, even if you think you know the sender; both could be phony. Instead, confirm with him or her on a different device and account that the message is genuine.

## 2 Look for signs that a webpage is secure and legitimate

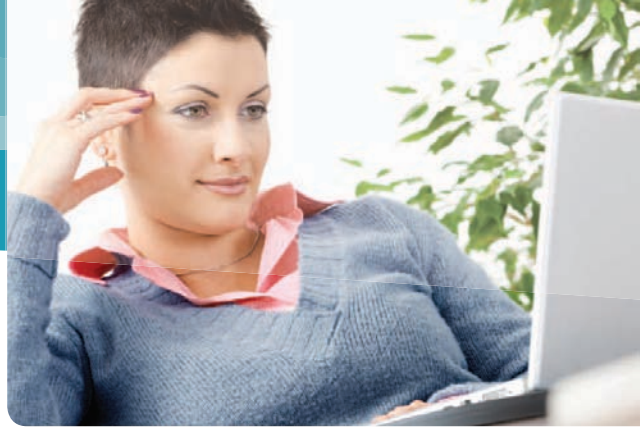
Before you enter sensitive data, check for evidence:

> Of encryption. 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.)




> That you're at the correct site—for example, at your bank's website, not a fake. One sign of trustworthiness is a green address bar like the one shown above.

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 email address and instant messaging name only with people you know or with reputable organizations. Avoid listing them on your social network page, in Internet directories (such as white pages), or on job-posting sites.

> Only "friend" people you actually know.

> Set the spam filters in your email service to Standard or High. In Windows Live Hotmail, for example, click **Options** and then **More Options**. Under **Preventing junk email**, click **Filters & Reporting**, and then make your choices.

## 4 Protect your computer and your accounts

> Boost your computer's security against phishing threats. Keep all software (including your web browser and spam filters) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Microsoft can help: **microsoft.com/security/pypc.aspx**.

> Don't use the same password everywhere. If it's stolen, all the information that password protects is at risk.

### More helpful info

> Get more ideas about how to keep spam out of your inbox. **microsoft.com/security/online-privacy/spam-prevent.aspx**.

> Learn more about identifying and protecting yourself from phishing scams: **aka.ms/onlinefraud**.

> Test your spam-spotting skills: **ilookbothways.com/spot-the-spam**.