

Computers Confuse Me

Bread Crumbs: [Home](#) > [Articles](#) > [Phishing Scams](#)

Phishing Scams

by **SCOTT GAWNE**

What is a phishing scam?

Simply put: A phishing scam is an email scam designed to steal your identity by tricking you into handing over your own personal information.

Phishing is a type of scam where the scammer uses fraudulent e-mails that appear to come from companies you trust, like your bank or credit card company, to steal your identity. Through this email, and most likely an imitation website to match, the scammer tricks you into submitting your personal information. This information is then used to steal your identity, opening accounts using your name.

An e-mail from a phishing scam can so closely resemble a legitimate business that it can be near impossible to tell it's a fake if you don't know what to look for.

How does a phishing scam work?

A scammer first creates an e-mail that mimics the financial institution of choice. They use a logo image from the website along with any other objects or features to make the e-mail look as close as possible to an actual email from the institution.

The e-mail will have a message that contains something similar to the statements below.

- Dear valued customer - they don't know your actual name.
- ... Please verify your account information
- Please respond within the next 48 hours or your account will expire/close.
- Click the link below to update your personal information
- ... System maintenance ... please updated your records
- Your account may have been compromised, please verify your information.

The email will typically try and portray some sort of urgency to get you to act on impulse. The email will probably ask you to either reply to the email or visit a link to update or verify your account information.

Following the instructions and entering your data sends your personal information directly to the scammer and they now have everything they need to steal your identity.

How can I protect myself?

If you receive an e-mail or instant message requesting person information do not respond or follow any of the links. | [more info ...](#)

Never give out personal information through email. | [more info ...](#)

Keep a close eye on your bills and statements to be sure everything is correct. | [more info ...](#)

Before giving out personal information across the Internet verify the site you are on is secure. | [more info ...](#)

Keep an eye on your credit report. | [more info ...](#)

How can I recover from a phishing scam or identity theft

To learn what steps you need to take to recover from identity theft read my "[How to recover from identity theft](#)" article

Phishing scam example

The screenshot shows an email with the following content:

Dear Flagstar Bank Member ^a

Due to recent account takeovers and unauthorized listings, Flagstar Bank is introducing a new account verification method. From time to time, randomly selected accounts are subjected to an advanced verification process based on our merchant accounts/bank relations and customer debit card.

Your account is not suspended, but if **in 48 hours** ^b after you receive this message your account is not confirmed, we reserve the right to **suspend you** ^c Flagstar Bank registration.

Flagstar Bank is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.

To confirm your identity with us click here.

<http://203.193.147.100/update/flagstar.com/onlineserv/HB/ANTIFRAUD/enroll/signon.htm> ^d

Please do not respond to this confirmation e-mail.

Sincerely,
Online Services Team.

What to look for:

- a) The bank would know your name
- b) and c) A sense of urgency to get you to act on impulse
- c) "suspend you ..." - bad grammer.
- d) Website is not www.flagstar.com or http://flagstar.com

Related links for further reading

- Wikipedia: [Phishing](#)
- HowStuffWorks: [How Phishing Works](#)
- Microsoft: [Microsoft: Recognize phishing scams and fradulent e-mails](#)
- FDIC: [Consumer Alert - Phishing Scam](#)
- [Related Blogs](#)

[top of page](#)