

YAHOO!

Don't Take the Bait

Phishing scams are e-mails or instant messages designed to fool people into divulging their personal or financial account information.

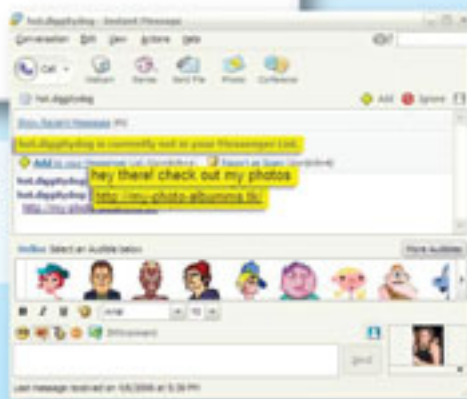


"Dear bank Client"

"To prevent deactivation, you need to submit the necessary information"

Anatomy of E-mail and Instant Messaging Phishing Scams

- Users should be wary of urgent or unsolicited e-mails requesting personal or financial information. Legitimate companies will never ask you to verify or provide any confidential information in an unsolicited email
- Instant Message (IM) users should be suspicious instant messages from people who aren't on your friends list
- Never reply to an e-mail or IM that appears to be suspicious. Suspicious e-mails or IMs are often generic in nature, and don't include your name or identifiers such as the last four digits of your account. They may also include spelling or grammatical errors.
- If you suspect an e-mail or IM may be fraudulent, don't open the message or click on links provided. Instead, log onto the website directly by typing in the Web address into your browser.



"Hot Diggity Dog" is not currently in your Messenger list

"http://my-photo-albumms.tk"

Greetings to U! Welcome back from summer break!

A handful of you have expressed an interest in learning about Internet security so you can protect yourselves from online scams like phishing. In this edition of U Asks Yahoo!, I will address your questions and pass along some pointers that will help you keep in touch with friends and family while you're away at school, studying abroad or even on road trips. I speak from experience when I tell you that there are all kinds of services out there that make it easy to keep friends and family close by, even when you're thousands of miles away.

As always, thanks for sharing your feedback with us and for asking interesting questions. We enjoy hearing from you. Feel free to e-mail me any Internet-related questions at askyahoocolleges.com and I'll do my best to answer them in upcoming columns.

—Ash Patel, Chief Product Officer

I've heard a lot lately about phishing. What is phishing and who's at risk? Is there anything I should know? What can I do to protect myself?

Phishing is a form of identity theft that baits consumers to share personal information like passwords, social security numbers or even credit card information via a spoofed e-mail or a fraudulent Website. Phishing attacks may come in the form of a fraudulent e-mail or an instant message containing a Web link and often exploit a trusted company or brand.

Many unsuspecting consumers have fallen victim to these scams by replying to spoofed e-mails and visiting fraudulent sites, so everyone is at risk. An estimated 2.42 million U.S. adults report lost money last year as a result of online phishing scams.

(continued on page 13)