

10 email scams to watch out for

Date: December 19th, 2009

Author: Debra Littlejohn Shinder

TechRepublic: A ZDNET TECH COMMUNITY

If it seems like you're getting hit with more email scams than ever, you're right. Deb Shinder explains what you and your users should watch out for to avoid being duped.

Spam is one thing. It's annoying to get email messages that are nothing but blatant attempts to sell you something. But other than using up your bandwidth, they don't really cause you any harm. Email scams are quite another thing. They aren't trying to sell you something; they're trying to steal something from you, con you out of or into something, or just scare you.

Email scams have been with us since the Internet went commercial back in the early 1990s. I remember getting those Nigerian scam messages back then. And believe it or not, they're still around. But scammers have gotten more sophisticated, and some of the more recent email scams are harder to detect — unless you know what you're looking for.

The holiday season seems to bring even more scammers out of the woodwork, perhaps because the average computer user is more vulnerable this time of the year. We're busy and in a hurry and may be less likely to notice the signs that a message isn't legit, and/or we're in a generous and giving mood and may be more likely to fall prey to a well crafted story that plays on our sympathy.

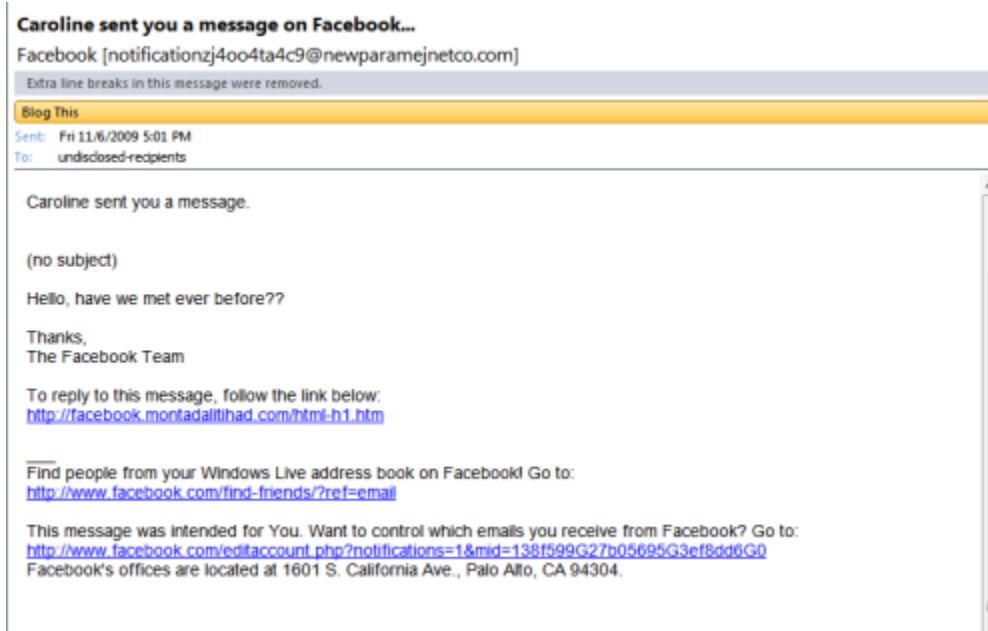
Let's look at some of the email scams that are currently going around the Internet and how you (and your users) can recognize them and keep from being victimized by them.

*Note: This article is also available as a **PDF download**.*

1: Fake Facebook "friend" messages

The popularity of social networking has surged, and scammers have jumped on that bandwagon to take advantage of the way the social sites work. For example, depending on your account settings, you may get email messages whenever someone posts to your Facebook wall or sends you a private message. Recently, I received a message with the subject line "Caroline sent you a message on Facebook." As with real Facebook messages, there was a link to click on to reply. But I get a lot of those messages, and this one didn't look quite right. **Figure A** shows the fake message.

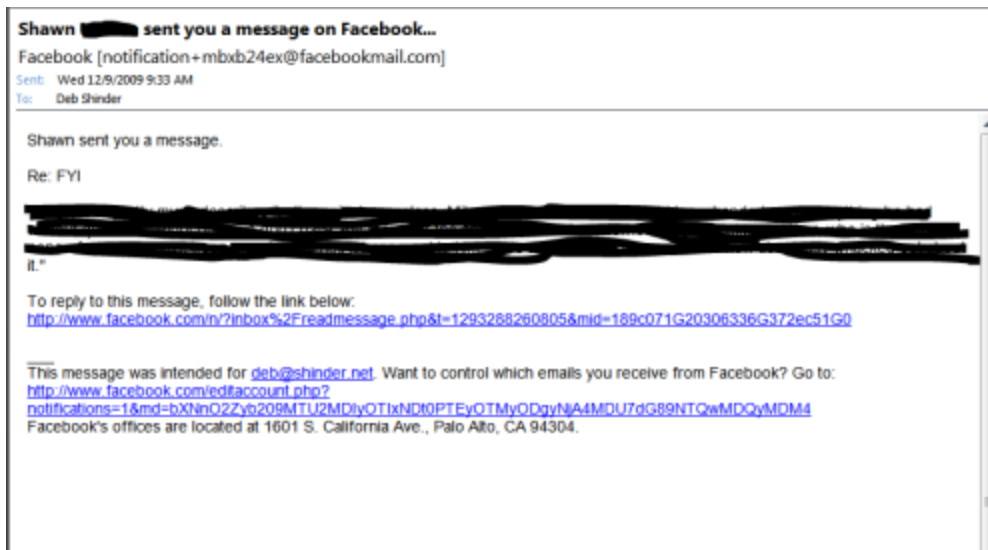
Figure A



Fake Facebook message is close, but not close enough.

I clicked back to a Facebook notification that I knew was real to compare the two. **Figure B** shows real message (with the content blacked out to protect the privacy of the sender).

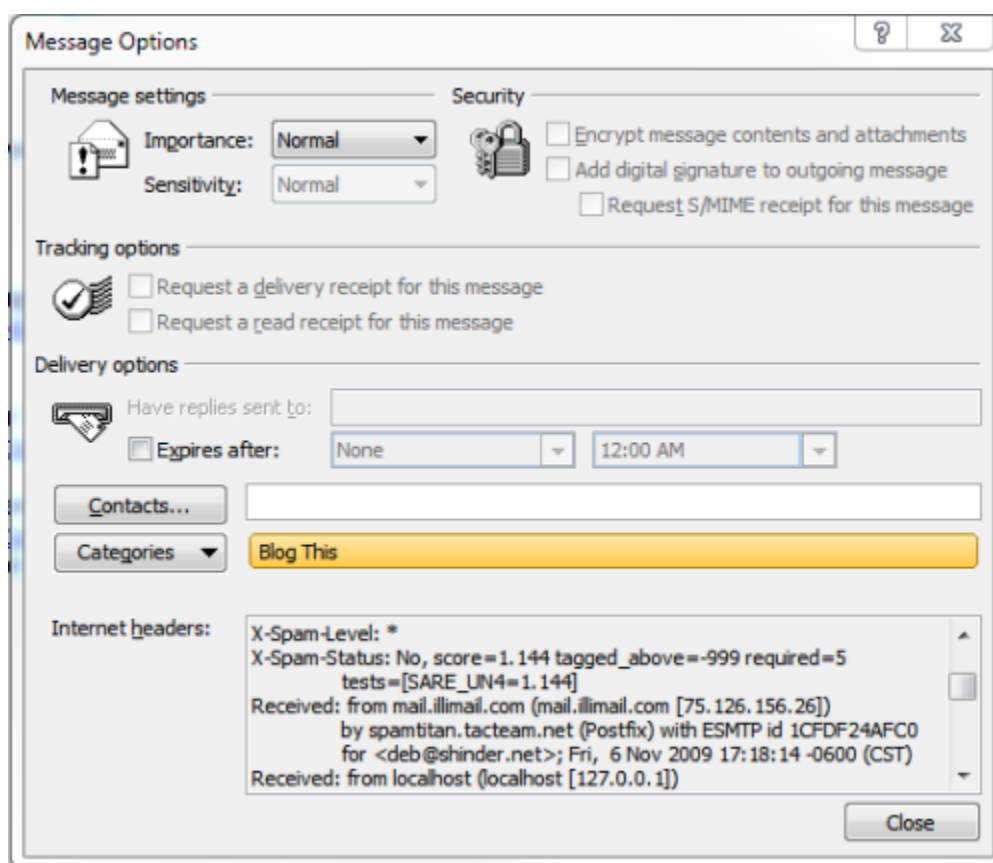
Figure B



The real Facebook message has subtle differences.

The first thing that caught my attention was the Reply To address. I expected the URL domain to be www.facebook.com, but the one in the fake message was facebook.montadalitihad.com. If you know how domain naming works, you know that means “facebook” is just the name of a Web server in the montadalitihad domain. As if that weren’t enough, I also noticed that the To field in the message didn’t show my name; instead it said “Undisclosed recipients,” indicating this message was sent to multiple people. All this was enough to cause me to check out the message headers (in Outlook 2007, you do this by clicking the Options icon. **Figure C** shows the headers.

Figure C



The Internet headers show that this message did not come from Facebook.

In a real Facebook message, the Received: field in the header would be from mx-out.facebook.com. In this one, it’s mail.illimail.com. Now I knew for sure that it didn’t come from Facebook.

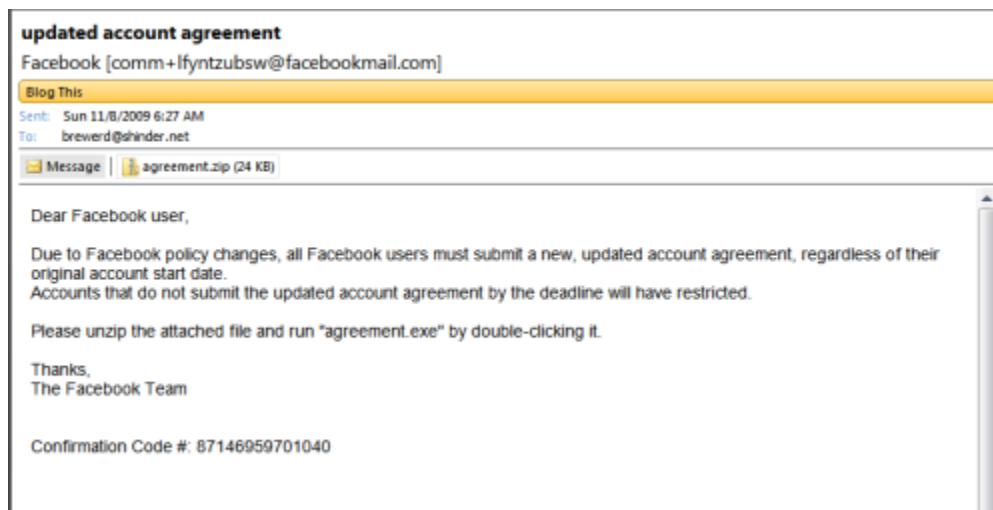
I had opened the message in a virtual machine, so if there was malicious code attached, it wouldn’t affect my real OS. Now I clicked the Reply To link and found that it opened a page that looks very much like the Facebook login page. The red

flag here was that I was already logged into Facebook with that Web browser. You should not get the login page if you're already logged into the service. I did *not*, of course, enter my credentials. That's the scam. If you do, the scammer will now have your Facebook user account and password and can hijack your Facebook site. Of course, variations on this scam may use other popular social networks, such as MySpace or LinkedIn. If you're in doubt about the legitimacy of any "friend" message, just log in to your social network account via your browser (*not* by clicking the link in the email) and check your Inbox. If the message is real, there will be a copy of it there.

2: Fake admin messages

You might just ignore a "friend" message (especially from a friend you've never heard of). But scammers know that a message from the site administrator is more likely to get your attention. This message pretends to be from "The Facebook Team" and purports to notify you of a policy change that requires you to submit a new account agreement. They try to scare you by warning that your account might be closed down or restricted if you don't do it. **Figure D** shows this message.

Figure D



Scammers up the ante by sending fake administrative messages.

This time, the scammer did a better job with the From name, which shows to be from facebookmail.com, just like a real Facebook message. But the first clue that it's a scam is the To address. That's not my name, and that's not the name of anybody in my domain. I have our Exchange server set up to forward messages to me when they're sent to nonexistent addresses (assuming they don't meet other spam criteria, which would block them at the server's spam filters). Spammers and

scammers often get hold of an email domain name and send messages to random names at that domain in hopes they'll hit on a real one.

The second warning signal is the attachment. Facebook agreements don't come as attachments; if this were real, it would direct me to a web page where I could read the new terms and click Agree. Attachments from strangers should always put you on alert.

I copied the attachment into a virtual machine and ran a virus scan on it. Sure enough, it was infected with a virus called VirTool:Win32/VBInject.gen!CN. Luckily, most antivirus programs that are up to date will be able to detect it. A check of the Internet headers on this message indicated that the Reply To address is somewhere in Germany.

3: Fear-mongering messages

While we think of scam messages as those by which the scammer profits, some don't benefit the scammer at all — except for whatever gratification a person gets from causing others to be upset or afraid. Unfortunately, this makes some individuals feel powerful.

There are many examples of these types of messages, and they usually seem to play on the current headlines. A few years ago, there was a flood of such messages warning that if you saw another car on the road at night with headlights off and blinked yours to signal to the driver, you were in dire danger of being shot as part of a gang initiation. This article details the **history of this email hoax**.

Similar fear-mongering scams have warned about a serial killer who lured women out of their homes by playing a recording of a crying baby and a rapist who would approach women in parking lots claiming to have picked up a five dollar bill the woman dropped.

The latest in fear-mongering messages like to play on health fears caused by all the recent media attention to swine flu (H1N1). An email message has been going around the Internet for several months warning that "The CDC says H1N1 is wiping out entire villages in Asia and expect it to hit the U.S. in January, where it will kill 6 out of 10 people." The message goes on to predict that martial law will be declared and you'll be shot if you leave your house to buy food, and urges recipients to stock up now and to buy face masks, use Purell, and take Enzacta products to "keep your immune system strong." If you weren't already a little suspicious, you probably will be by the time you get to the end, where the sender says the pandemic was predicted years ago by a Russian mathematician and that it was caused by a tsunami. Here's **the full text of the message**.

They always say that if something seems too good to be true, it probably is. The same goes for over-the-top bad news — especially if you're hearing it for the first

time in an email message. You can bet that if the CDC had really put out such an announcement, it would be all over the mainstream news outlets.

4: Account cancellation scams

It seems that around the holidays, more of these than usual start popping up. I've received a number of messages telling me that my account has been or is about to be cancelled — purportedly from Amazon, PayPal, even from the bank. Close examination of the messages show them all to be bogus. Of course, in many cases, I already knew that, because I don't even *have* an account with the organization. Here's another clue: The message contains a link that looks legit, such as www.mybank.com, but when you hover your mouse pointer over it to show the actual URL, it's something different, often with a foreign country code such as .ru (Russian) or .cn (China).

Still another clue is that these scam messages often contain typos or grammatical errors you wouldn't expect from a legitimate company.

5: Bogus holiday cards

There are numerous Web sites through which you can send virtual holiday cards to your friends, and many people take advantage of this quick and easy — and inexpensive (no postage stamps required!) — way to send season's greetings at this time of the year.

Scammers have co-opted the idea, though. They know that many computer users won't think twice about clicking a link to view a card from a friend, so they send out messages notifying you that you've received a card, with a link to a Web site that will download malicious software to your computer if you aren't properly protected. So how do you tell the real card services from the scams? For one thing, when a friend sends you a card from a real service, it will almost always tell you the name of the sender. Scam messages are more likely to use the generic "A friend sent you a greeting." The safest way to check is to do a Web search for the card service and read about it to find out if it's a legitimate one. Or to really be safe, just ignore the card notification and send holiday greetings to your friends the old fashioned way (through the postal service) or by personal email, instead of using a Web service.

6: Phantom packages

Any other time of the year, you might be suspicious if you were notified that you had an unexpected delivery from DHL, FedEx, or UPS. During the holidays, it's a common occurrence. Scammers know this, so they're seizing the opportunity and

sending email messages telling you that you have a package that couldn't be delivered because of some problem with the shipping address.

This particular scam contains an attachment that's supposed to be a form you need to print and fill out so you can pick up the package. However, there is no package and when you open the attachment, **it infects your computer with a virus.**

Also beware of variations on this theme. Many people know not to download email attachments, but they'll readily click a link to go to a Web site. So more sophisticated scammers will send you to a site that looks like that of the delivery service, but that delivers only malware — straight to your system.

7: Threats from the government

A sharply divided partisan political system has resulted in a growing distrust of government in many circles. Some scammers are now playing on those sentiments. A recent scam email has been going around that purports to warn you that the Department of Homeland Security and the FBI have been informed that you're allegedly involved in money laundering and/or terrorist activities. The email goes on to say that you can avoid prosecution by obtaining a certificate from the Economic Financial Crimes Commission Chairman — for only \$370. Who wouldn't jump at that deal?

Many similar scams use the names of government agencies. Of course, they're all hoaxes. If you were really the target of a DHS or FBI investigation, you wouldn't be able to buy your way out of it for a few hundred bucks. And those agencies would be contacting you in person, not sending threatening email messages.

8: Census survey says...

Another recent email scam also involves the federal government, but instead of accusing you of a crime, it uses your knowledge of real, routine government activities against you. Everyone knows that the U.S. government conducts a census every 10 years, and 2010 is the year. Citizens are required by law to answer the census-takers' questions. Most people also know that many government-related tasks can now be done online.

Scammers are taking advantage of this to send phishing emails that claim to be from the Census Bureau, making it "convenient and easy" for you to fulfill your census obligation, either by filling out an attached form and emailing it back or by visiting a Web site to fill in a form. The form asks for all sorts of personal information, including the social security number and date of birth of everyone in your household, which can be used for identity theft.

In addition to asking you these personal questions, the emails may include attachments containing malicious code that can infect your computer. The same goes for the Web links contained in the email message. The Census Bureau does, in

fact, send **email regarding your participation in a survey** — but it does *not* ask for detailed personal information.

9: In Microsoft (or Apple or Dell or HP) we trust

There are dozens of email scams out there that attempt to exploit users' trust in the vendors that make their computer software or hardware. **These messages say they're from the vendor** and range from fake security warnings with attachments that claim to be vulnerability fixes (but are really malware) to bogus "special offers" to "payment requests" that require you to download and install a "transaction inspector module" (which is really a Trojan) if you want to decline to have the payment charged to your credit card.

10: You're a winner!

There are many new twists on an old theme: You're a winner in the lottery, contest, or drawing. All you have to do to claim your prize is fill out a form and email it back. Of course, the entity awarding the prize needs your social security number because the value of the prize must be reported to the IRS.

The bad thing about this scam is that you *will* indeed have to provide such information to claim a prize in a legitimate contest. As a Microsoft Windows 7 Launch Party host, I was automatically entered in a contest to win a Dell laptop — and I won. When I got the email notification, you can bet I was suspicious. Before doing anything, I checked it out with my contacts at Microsoft. Even after confirming that the notice was real, I declined to send my personal information back via email; I printed out the form and sent it via snail mail (registered and certified) instead.

Even if you really did enter the contest that you're being told you won, don't get careless. Check into the legitimacy of an email notification of the good news. And I recommend never sending your social security number or other sensitive information in unencrypted email. A legitimate contest will almost always have alternatives methods by which you can submit your information