

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

Guarding Against Email Scams

By Susan Dunn

Guarding Against Email Scams by Susan Dunn, Marketing Coach and Consultant

The email scams aren't going to go away. Our only recourse is to stay ahead of the game by learning its rules. The way to do this is using the Emotional Intelligence competency of intuition. Intuition is not some "mystical" thing; it's the result of experience and processing, and then getting mindful about what you've learned that you aren't initially aware of. There is always something "odd" about these emails. Stay alert and follow your instincts. Intuition is knowing, rather than thinking.

One type of email scam is designed to get secure information from you - and who knows what else. I haven't replied to any, so I don't know what else is involved. I don't want to know, and you don't either. The least innocuous result would be getting your email address on some mailing list. The worst-case scenario? Viruses, hardware crashes, identity fraud, access to your account and money, and who knows what else.

If you have an Internet business, or spend a lot of time on the Internet, as I do, and receive hundreds of s*** emails per day, you learn to recognize the signs. (Intuition is really a matter of lots of experience and paying attention to the "signals" which alert you that something is amiss.)

If you do business on the Internet, as I do, likely you have a PayPal account. This latest scam sends you an email warning you that your PayPal account is about to expire, and requests information, or requests that you go to a site to update your information. (I have recently been receiving these allegedly from ebay as well.) As you know, PayPal says they will never ask you for this information via email, and they warn you not to give it.

Pay attention, because it's very easy to copy someone's logo, font size and color, etc. off the Internet, and at first glance it can look just like the site it's imitating.

How do you recognize the scam email? I'm both sorry and delighted, as an English major, and champion of proper English, to say that one of the signs of a scam email is poor English.

SUBJECT LINE

Guarding Against Email Scams

First of all, the subject line is almost always peculiar. The latest one I received reads "YOUR PAYPAL.COM ACCOUNT EXPIRES." No one would write this way. More likely it would say "Important information about your PayPal account," or "Notice about account" or something like that. Who writes subject lines in all caps? It's also in the wrong tense. Your account WILL expire, or IS GOING to expire, yes?

BAD ENGLISH

Within fake messages I have always - ALWAYS - found typos and grammatical errors, and I mean blatant ones. This particular email contained: "To avoid any interruption in PayPal services then you will need to run the application that we have sent with this email (see attachment) and follow the

instructions." "Then" doesn't belong in this sentence.

Skim through the email and you will find bad English. I mean far worse than usual!

SIGNATURE LINE

The signature line doesn't ring true either. Use your intuition. I have received some that said "Benjamin Smith, Director of Services, blah blah." Nowhere on the PayPal site will you find anyone's name of position within the company ... will you? One of the feelings we all have about the Internet is that anonymity, and it holds true. Who "runs" amazon.com? I mean what person?

Another sure clue is those odd words or letters at the bottom. I've tried to find out what purpose they serve (to the perpetrator, I mean) and haven't been able to, but if they're there, there's your clue.

In this case the email is signed:

"Thank you for using PayPal.

>

> zapzevoe"

At other times there are several lines of letters running across the bottom.

FAKE WEBSITE

Other emails will tell you to go to a URL to give information about your account. It will not be www.paypal.com or <https://paypal.com> but something else. Often it is a site with PayPal listed at the end, like www.xxxxxxxxxx.com/paypal.htm .

DON'T GET CURIOUS

Pay attention to when you feel something's suspicious, but beyond that don't get curious. What are these people after? I don't know, and I caution you not to be investigate. Just delete the email or forward it on to PayPal (see instructions below). Don't go to the spoof site they list, or open the

attachment, or reply to the email.

If you are in doubt, call the business the email is allegedly from. In this case, if you go to the PayPal site, you will see ample information about fraud and protection of your account. Included is the advice that you go to paypal and log in: <https://www.paypal.com> . Also that you report any possible spoof email or fake websites by forwarding the email to spoof@paypal.com . You can go here https://www.paypal.com/ewf/f=sa_fake to report a fake as well. PayPal tells you how they will request information from you, for instance, using your first and last name, and that they will also request you go to <https://www.paypal.com> and login. If you use a service such as PayPal, be sure and check out their anti-fraud information.

Lastly, here are two numbers where you can reach PayPal: 1-888-221-1161 and 1-402-935-2050 should you wish to talk to someone.

In sum, look for these clues re: fake email and when in doubt, call the company, or simply delete the email without responding to it:

- Strange subject lines
- Your first and last name are not used
- Grammatical errors, typos and misspellings within the body of the email
- Letters strung out at the bottom of the email

©Susan Dunn, MA, Marketing Coach and Consultant, <http://www.webstrategies.cc> . Our goal is to help your Internet business succeed. Web strategies, search engine placement, articles written, article submission, web design, and marketing plans. [Mailto:sdunn@susandunn.cc](mailto:sdunn@susandunn.cc) for free ezine. Put "Checklist" for subject line.

Email Spam and Phishing

By Radha Khalsa

It seems like the volume of email spam has doubled in the last month. Increasingly, we receive daily emails for better mortgage rates, pharmaceutical discounts, and offers to enlarge body parts we don't even have.

The next generation of sophisticated tools is available to email spammers. Hidden code can be embedded into email allowing the sender to track it. A "spam beacon" lets the sender know that this is a valid, live, email address. The sender can also tell if you've opened the email before you tossed it. "Nearly half of all spam is bugged with so-called "spam beacons" for tracking users who open junk mail, said e-mail filtering firm MX."

The latest email scams have also evolved. The newest scams are called phishing attacks. Spammers copy and paste web coding, making their email message appear to be official. They provide links to "look alike" websites where they try to trick you into revealing your personal financial information, by

Guarding Against Email Scams

asking you to update an account such as Ebay, PayPal or CitiBank (or other well known entities). Phishing attacks are successful 5% of the time.

The primary motivation behind these emails is identity theft. Scammers are looking to get you to their website and get your information. If the authenticity of the sender is questionable, call the company that sent the email. Most business email will also contain a phone number.

Earthlink is trying to address this problem by releasing new software. Its latest anti-spam software is available to both members and non-members. The software installs with Internet Explorer and automatically downloads a list of known "scam" websites. If you surf over to a site on the list, you will receive a warning.

Given the large volume of unsolicited email that must be sorted through and deleted daily by businesses, do not rely on email as your primary vehicle of communication. If the information is time sensitive, it's best to follow up with a phone call.

MARKETING COORDINATOR and WEBSITE DESIGNER—Radha Khalsa, has extensive experience in the areas of marketing analysis, strategic planning and project management.

Email Spam and Phishing

Watch Out For eBay Automobile And Computer Scams.

Five Scams You'll Want To Avoid

Email is great! Or IS it??

How To Get Rid Of Spam Stock Market Tips

Scams Exposed

Email Spider Software

How to Buy a Car Without Getting Ripped Off!

Newbie's Guide to Stop Spam

Instant Email Scramble



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!