

YOU SHOULD BE SUSPICIOUS

Things to be skeptical about in email

Apologies

If you own a home that is mobile
and five cars that aren't...

...you might be a redneck.

—Jeff Foxworthy

Healthy skepticism

The Internet is a place that is wild and free, and a little dangerous for the unprepared. It's easy to look at apparently professionally-crafted messages and web sites and forget that they cost very little, can be created by people who are effectively anonymous, and who may reside in a place where US laws can't touch them. Unfortunately, these aren't all nice people.

You need to learn to “be careful out there.” This tutorial should help you begin to figure out what to look for.

Me? Really?

If you receive a message threatening to close your account at Second National bank of Decatur, only you don't *have* an account at Second National bank of Decatur...

...You should be suspicious.

If you don't understand *why* a message came to you, maybe it's because it's fake.

Just for me?

If you receive a message that is about some special offer or some situation that applies to you and you alone—but the message is addressed to fifty people (or “undisclosed recipients” rather than just you)...

...You should be suspicious.

A message that's just *for* you should be sent just *to* you, and not as a carbon copy.

Do I know you? (Do you know me?)

If you receive a message asking for personal details about you and your account, but the sender can't be bothered to address you by name or specify which account he's talking about...

...You should be suspicious.

If the sender doesn't *seem* to know anything about your relationship, maybe it's because he doesn't.

Who are you again?

If you receive a message about a FedEx delivery, and all of the links point to pizzahut.com...

...You should be suspicious.

If a message claims to be about one company or service, but the “from” address or the links go to a different company or service, something’s not right.

You're where?

If you receive a message from an official US Government Agency, and the links go to **us.gov.ru** (a web site in Russia)...

...You should be suspicious.

If the domain ends in a two-letter country code, it's worth Googling "list of TLDs" to see where it is. You might be surprised.

Only one way out

If you receive a message with a variety of links for different parts of an organization's web site, yet they all have exactly the same web address...

...You should be suspicious.

A link labelled "Contact Us" should probably not go to the same place as a link labelled "Catalog"; If all the links go to the same place, something's up.

Calm down, Chicken Little

If you receive a message promising that all sorts of dire things will happen if you don't respond **immediately**...

...You should be suspicious.

Email is not a high-priority Internet service. Delivery is not guaranteed, and can be delayed up to five days. If it's really *that* urgent, the sender should contact you another way. **(Take time to think.)**

You want what?

If you receive a message demanding that you send your house keys, your car keys, and the alarm codes...

...You should be suspicious.

Seriously: passwords, credit card numbers, and other personal details would be just as damaging in the wrong hands. Why would you share them with anyone? Over email?

Your mask is slipping

If a message from a big corporation, a government agency, or a reputable university can't distinguish between "being fit," "getting fitted," and "having a fit"...

...You should be suspicious.

Messages with *multiple* translation errors, misused idioms, poor grammar, and spelling or punctuation mistakes may indicate that the sender is not a native speaker of English (and just maybe, not who he says he is). Genuine large organizations would probably catch most of these in proofreading before sending the message.

I won, I won!

If the message tells you that an amazingly wonderful opportunity has just come up for you to make a lot of money with almost no effort...

...You should be suspicious.

Winning lotteries you never entered, helping people you don't know to move inheritances or lost fortunes across international borders and getting rich—if it sounds too good to be true, it probably isn't. (You wouldn't trust a bum on the street; why trust a bum on the Internet?)

So I'm suspicious. Now what?

Most important is what **not** to do:

- ❑ Don't reply to the message.
- ❑ Don't click on any links in the message.
- ❑ Don't open any attachments included with the message.

If you are really unsure of what to do, call the Help Desk at 610-758-4357.

Otherwise, just delete it. (And have a nice day!)