An email from your Bank – or is it?

Check the sender's address BEFORE opening an email

Yes, this does look like the previous Internet Tip which is why I haven't changed the sub header; and I realise it might seem tedious to keep harping on about the issue; but, judging by recent media warnings, the problem is rife and increasing. In fact, only the other day we had an email claiming to be from our bank and stating that our account had been suspended. The content and whatever it suggested was required to be done by us remains unknown because we declined to open it. What we did do was take a walk to our local branch to ask the obvious question and were told: "No, this is not from us: the Bank does not conduct business in this way." Having informed them of the bogus email, we left it to them to take whatever action they deemed necessary.

This is not an isolated case. A number of similar deceptive emails show up regularly on our spam list. The majority are disregarded and deleted, particularly when the named bank or company is not one we do business with. Those that are of concern are like the one mentioned above, and I suspect that some Internet users could be duped into responding, believing the communication to be genuine. Should you be tempted, please hold off opening these fraudulent emails. Instead, action them the way we have by contacting the Company's on-line service (not the one on the spam list!), phone them, or pay a personal visit and talk to a real person over the counter. Then you'll know the truth.

I am not scare-mongering here – there are risks contained in these emails. If you do take a chance and open one - BEWARE! They may claim your personal or banking records need updating – DON'T GIVE THEM ANY DETAILS! Your identity could be stolen, or your account stripped. If the message is bullying or threatening - DON'T BE INTIMIDATED! Just close the email and contact whoever it is supposed to be from. If there is a link to click on – DON'T DO IT! The moment you arrive wherever it takes you, the door is open for bugs and malware to enter your system – from Trojan Horses which sit dormant until eventually activated causing havoc or inconvenience; to a code which locks up your computer, then delivers a ransom demand to unlock it.

Whatever you do, take this very seriously. And don't believe that you are of no consequence to these frauds and tricksters because you are simply an ordinary person. That's precisely the reason you are targeted. You seem to be less likely to take the matter further than someone with power and influence. Well, in this instance, you do have the power – to ignore, to delete and to report to a higher authority which hopefully has an arm long enough to catch these predators.

Take a look at Internet Tips IT10 for easy ways to check the authenticity of anyone sending you an email BEFORE YOU OPEN IT!

Return to the Web Page to read, download and print information on a variety of topics