By Adam Levin, chairman and co-founder of credit.com and Identity Theft 911

For many people, the first sign that their email has been hacked comes when a friend shoots them a text or an email saying, “Hey there. Uh… I think your email was hacked… unless you meant to send me that link to the Viagra store.” Or you might figure it out because you can no longer log in to your account, or your smartphone can’t retrieve your messages. Or maybe you can log in to your email, but find that your inbox is suddenly empty and all of your contacts have been deleted. No matter what tips you off, when your email is hacked (notice I say when, not if, here), the impact can be disastrous.

The fact is, despite Twitter, Facebook and texting, we still rely on email for most business and personal interactions. So it can be pretty disquieting when inexplicable things start to happen to our email accounts, or our access to email is blocked. When these things happen, we can’t just will them away or delude ourselves into thinking that our computer is simply having a bad day. They could well be manifestations of email hijacking, which often is the prelude to identity theft. So your response should not be “Oh God,” but rather, “Houston, we have a problem.”

There are plenty of things you can do to minimize the risk of having your email hacked, as we’ve covered in the past. And if you’re worried about how to spot suspicious emails in your inbox, there are plenty of telltale signs. Nevertheless, these days nothing is foolproof and nobody is perfect, so the likelihood that you will be exposed to a phishing scam at some point is relatively high. The question is what you do when it does eventually happen, to keep both you and your friends safe. With that in mind, we offer these tips:

1. Change your password.

If the wizards who hacked into your account forgot to change your password and you can still log in – do it immediately and change that password. Oh, and make it stronger, stranger and less “you.” That means no birthdays, addresses, kids’ names, dogs’ names, maiden names, favorite movie names, favorite band names, or anything else that you might otherwise feature on your Facebook page.

2. Recapture your account.

If your access is blocked, follow the directions on the email site help center. Once you again become the master of your email kingdom, invent a very sophisticated password, change your security questions and get creative in your answers because the hacker may well have nailed those questions correctly in the first place. Trust me -- you want them out of your life and not as permanent pen pals.

3. Report the incident to the email site.

Your email provider has seen this type of thing before and may be able to provide you with further details about the nature and source of the attack, as well as any tools they may have available to protect your information and get you back up and running. (You may also have access to identity protection services through your insurance company, bank, credit union or employer).

4. Speak to your peeps.

Notify everyone on your contact list that you have been compromised and they should look at any communication from you with suspicion for the time being. Further, they should double down on their computer protection. If they have already been victimized, offer your condolences and support, and make sure they are following these steps, too. (Hey, maybe forward them THIS article!)

5. Scan your computer with an updated anti-virus program.

Don’t think that sophisticated email hackers are in it for the fun of grabbing your email and then doing a spam conga line. Often their goal is much more insidious. Why crawl into a life unless you can truly monetize it? Therefore, beware of the Trojan. (As a Stanford guy, that has always been my motto when dealing with people from USC.)

In this case however, they may have inserted it into your system so that it can conduct recon and report back to them with all of your passwords or a treasure trove of your information. Get that program running and eliminate any and all viruses, spyware or malware that it discovers. If you don't have a new and sophisticated security software program now is not the time to cheap out. It's a reasonable investment that will ultimately show a serious return by keeping your information yours.

6. Don't fail to review your personal email settings.

Make sure the cyber ninjas haven't created forwarding email addresses and if you find any delete them immediately. Also, look carefully at the signature block and make sure it's really yours. The hackers may have included some malicious links there too.

7. Change passwords or security questions for other sites.

In the event you shared your email passwords or security questions with any other site, change them, too. Too often consumers opt for convenience (or simplicity) over security and use a single password for multiple websites -- including financial services, social media, retail or secondary email sites. Not a good idea. In fact it's a very bad idea. Change all of them and use different passwords for each.

8. Check your email folders.

Folks have a tendency to send financial or personally identifiable information to others via email and then archive the offending email in a file in their system. If so, immediately go to whatever account is identified and change the user ID and password.

9. Monitor!

Assuming that the hacker in question was able to find either your Social Security number or

other valuable pieces of personally identifiable information, it will become important for you to monitor your credit and various financial accounts for suspicious activity. You can start by contacting the fraud department of one of the big three credit reporting agencies and having a fraud alert put on your file, and you may even want to ask them to "freeze" your credit. If you think you may be a victim of identity theft, you are entitled to a free copy of your credit report from each of the three major credit bureaus. You also have the right to request a free credit report from each of the bureaus once a year, whether you are a victim or not.

Your email is an important component of your identity portfolio. You must manage it like an investment. That means you minimize your risk of exposure by being smart, discrete and sophisticated in your security approach; keep a watchful eye for things that seem a bit “off,” and know what your damage control options are before you need to control the damage.