

Be suspicious online

I don't have to tell you that identity theft is a big problem in today's highly connected society. I also don't have to tell you that cybercriminals feed off of our private information. Now, given that our private information is so vital to their mere existence, it stands to reason that they are going to find a way to acquire it.

These thieves can go about it the hard way, such as actually hacking into your accounts, tapping into your network or physically stealing your computer. Or, they can go about it the easy way, which in fisherman terms, is to cast out a



Nancy Victor: She is the Help Me!! Tech Team president.

GUEST VOICES

great big net to catch naïve victims to see who actually might hand them the information they require.

To protect oneself from the "phishermen," you must first understand what "phishing" is.

Phishing is a way of attempting to acquire private data such as a person's username and password, credit

card information and/or account numbers by masquerading as a trustworthy entity. Phishing is typically carried out through email or text message, and it often directs the user to enter details at a fake website that looks almost identical to the legitimate one.

The first thing to know without question is that no legitimate financial institution ever would lose your username and password nor would it send you an email requesting that you update your account information.

See GUEST/4C

GUEST

CONTINUED FROM 1C

The same can be said for Facebook, eBay, Amazon or any other site you may have joined or from which you have made purchases.

Legitimate companies might send you an order confirmation, but only after you have ordered

something. They also might send you a "thank you for joining" email after you sign up.

Pay close attention to emails that confirm a password or username change. These requests are a little harder to ignore. In fact, you very well may have just engaged in these very things. Remember, good timing and gullibility are what "phishermen" are

hoping for, but there are some rules of thumb that will help keep you out of their nets.

First is action. When you receive any email asking you to respond in some way, DO NOT click on the link provided within the email. Instead, go directly to the site yourself. This will ensure that you have gotten to the legitimate site and not the fake phishing site.

Once there, look for the `https://` in the URL before entering in information that you prefer be kept secure. Keep in mind that security questions are helpful to include when you set up new accounts and be sure to always use complex passwords that include a mix of numbers, letters and special characters.

Second is avoidance. Enlist the help of an email

filtration device that will help weed out many of these phishing emails and spam in general.

This piece of hardware is especially helpful to businesses that receive email messages in greater volume. It lowers the risk by catching most spam, phishing and virus-infected emails before they ever reach the user. It also keeps your inbox clean and keeps your network

running proficiently.

Finally, embrace your inner skeptic and second-guess everything you receive in an email or text message — including items that appear to come from a friend or your friendly neighborhood banking institution.

Nancy Victor is president of Help Me!! Tech Team, a 20-year systems integration firm serving San Antonio.