Tips for Staying Safe on the Internet

November 3 2005

Dan Barker, the co-owner of Strategic Data Integration in Hillsborough, N.C., and an editor of “Certified Internet Webmaster Foundations for Dummies,” teaches the Duke Continuing Studies course "PC Threats: Spam, Scams & Viruses". He recently spoke with Stuart Wells of the Office of News & Communications about computer safety.

Q -- In recent weeks, we’ve seen post-Hurricane Katrina online scams, “free credit report” sites that have put people at risk for identity theft and continuing reports of Internet “phishing” scams. How pervasive are online scams and are crooks using ever more sophisticated schemes to cheat unwary computer users?

A -– It’s the same kind of problem that we’ve had with junk mail and with phone calls. You never really know who’s calling you. Depending on whose numbers you look at and how it’s measured, 10 to 80 percent of e-mails are fraudulent. And, in my mind, you can lump together these same schemes with spam. They’re trying to get you to buy something that isn't real or to get your e-mail address.

Several U.S. agencies are looking into it, but tracking down the sources is still very difficult. There are ways to track it, but it requires the cooperation of all the countries involved. And, in some countries, it is government officials who are profiting. Some Chinese officials, for example, maintain server farms and those are used to launch many frauds.

In the case of so-called ‘419 spammers,’ you get an e-mail from someone who says he is the president of some African country who has tucked away money somewhere and if you give him $1,000, he'll send you back $2,000.

The problems are not necessarily increasing, but more people are realizing that they've been taken. Perhaps in the past you would get an e-mail you didn't understand and would delete it, but more of us now realize it's fraudulent.

The real problem is that people respond to the e-mails. I have a friend who doesn't understand that it may not be a good idea to click on an 'unsubscribe' link because that will tell them they've reached a warm human body.

What we're seeing is not really more sophisticated. It's still at the level of the traditional bait-and-switch or basic confidence trick. Those have been around for a few centuries.

Q -- Is there any simple way to verify that the e-commerce and other sites you use are actually who they say they are?

A -- There are tools to look up a domain name and find out who owns it and where it's based and if it's from a country that has a reasonable legal system. You can also type in a made-up account number. If the website is truly connected to the world banking system, the webpage will show the error immediately.

Also, you should be able to contact a legitimate website by e-mail and expect a response.

The main thing I would advise is to not use your primary e-mail address, but to use a secondary or temporary address that you can obtain from mailexpire.com, mailinator.com or cruelmail.com. This allows you to filter email using a human challenge system.

A more controversial group, bluesecurity.com, allows subscribers to download software and report spammers. They contact the offensive e-mailer, who gets large quantities of e-mail in return if they persist in e-mailing Blue Security members.

Anyone who owns their own domain name has another way to fight the spammers. A domain name gives you the option of using a slightly different e-mail address with each online company you contact and you can quickly see if someone has sold your address to a third party. I've seen a few of my own e-mail addresses spread among spammers. It happened when BMG Music's mail list was stolen.

When visiting an e-commerce website, the pages where you enter your personal information should be secure. You can tell the security through visual cues in your browser. Secure websites purchase a digital certificate that guarantees who they are. When this certificate arrives at your computer, it is compared to the information that the company that issued it has on file for that site. If the two agree, that is a fairly good assurance the site is who they say they are and that anything you send to them will be secure. Browsers display a golden padlock or golden key in the bottom status bar of the browser window when a valid certificate is received. The address for the site should also begin with https:// instead of just http://. If you go to a website that has an invalid certificate or for which the site name does not match the name in the certificate, your browser should warn you that the certificate is wrong. The X.Com website is now owned by PayPal, so if you go to www.x.com, you should get the security warning that the domain name does not match the certificate name.

When the golden padlock or key is displayed, you can double-click on it and see the information about what corporation owns the certificate and website. All major browsers released since the mid-1990s have the https, technically the Secure Sockets Layer security option. There have been ways to fake the browsers into displaying the golden padlock with weak security, but current Windows and MacOS patches block those problems.

If you do not turn off security warnings in your browser, they will give you very good information about when you are entering or leaving secure websites. Many people are tempted to turn off the warnings that browsers give. I usually recommend that you leave them on, or restore the warnings to the default levels until you understand what the warnings mean and can decide for yourself which ones are important to you.

Q -– What’s the one best thing a computer user can do to stay safe on the web?

A -- The best thing is to treat the Internet as if it’s a bunch of strangers. Don’t give out any personal information until you know who you are dealing with.

In the non-computer world, most people would want to be able to make a phone call to the person. In the virtual world of the web, it’s reasonable to ask for a phone number and then you can call them and confirm that they're a real person.

Many people have huge fears of what could happen to them on the Internet, but are unaware that choosing an English word as a password is still the biggest problem since a hacker will take a dictionary and try popular password words with common user names that people use. Taking the simple step of adding a digit in either or both your username and password will make you much safer on the Internet. Many banking sites, and universities like Duke, are requiring these stronger usernames and passwords for systems with sensitive information.

Q -- In your view, is enough being done by government to protect the public from fraudulent websites?

A -- I don't think this is an area where the government necessarily needs to be more involved. But they do need to provide a better way to receive fraud complaints. North Carolina does stand out for having a complaint form that's easy to use even though the offense may not be one that can be prosecuted here.

Source: Duke University

Citation: Tips for Staying Safe on the Internet (2005, November 3) retrieved 18 April 2024 from https://phys.org/news/2005-11-safe-internet.html