10-17-2016

Recognizing and Combating Cybercrime

Marcia L. Dority Baker
University of Nebraska-Lincoln, mdority_baker2@unl.edu

Why IT Matters to Higher Education
EDUCAUSEreview

https://er.educause.edu/blogs/2016/10/recognizing-and-combating-cybercrime

Recognizing and Combating Cybercrime

Authors: by Marcia Dority Baker
Published: Monday, October 17, 2016
Columns: Security Matters

Can You Spot the Scam?

Scams make great stories. Tales of Internet crime or other fraud make up some of Hollywood's most exciting thrillers. While cybercrime blockbusters are fun to watch on the big screen, cybercrime is a serious problem on campuses globally.

How many people do you know who are the victim of a scam (Internet or phone)? According to the FBI, cybercrime is a growing threat that affects individuals and businesses around the world. A recent *Washington Post* article reported that cybercrime cost the global economy $445 billion in 2014.

What Is a Scam?

A good way to understand **what** something is is to know **how** it is defined. This post will use the Wikipedia definition of *Internet fraud*:

The use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

We need to think of scams, fraud, and cybercrime as synonymous. There are many words to describe this topic but each have at their core the sense of financial deception and all refer to the same concept: to take advantage of someone or — to use an old verb — "to swindle."

Who Is on the Other Side?

Remember the *New Yorker* cartoon, "On the Internet, nobody knows you're a dog"? This is one of my favorite cartoons and a perfect example of how a picture is worth a thousand words. While this cartoon came out in 1993, it holds very true today. On the Internet, it is easy for users to hide behind an alias, to share half-truths on a product, or to push a false service to gullible users.

Too Good to Be True

If it sounds too good to be true it probably is! Our ever-changing technology makes gathering information easier, especially as Internet users readily share personal information online. The challenge to outsmart the bad guys is a struggle for all organizations and individuals. We must stay informed of current trends in cybercrime to educate our campuses (faculty, staff, and students) on best practices for sharing content online and protecting valuable information. The FBI maintains a resource list of common fraud scams including examples of each type of scam and tips for staying safe online. This is not an exhaustive list of scams — as technology evolves, so will fraud.

Commonsense Approach

"Everybody gets so much information all day long that they lose their common sense."
— Gertrude Stein

The constant flow of information combined with changing technology can leave users feeling overwhelmed. Below are several suggestions for evaluating resources, sharing information online, and staying safe.[1]

- The first step is to determine the scope of your online presence — both personal and professional. This will assist in finding and fixing any potential information leaks. Internet users should create an inventory of where personal information is available online (e.g., see my inventory list). Any website that requires an online account with username and password **and** can store credit card information should be added to the list. This inventory includes the usual sites such as social media and gaming as well as online pay sites provided by banking, health care, household utilities, and credit cards. Don't forget to add membership sites such as Netflix, iTunes, and online pay sites that previously took a check. Many Internet users are surprised at the size of their digital footprint; the convenience of online pay, record keeping, and purchasing requires the sharing of personal information in a wide variety of places.

- Do not share pertinent personal information online such as Social Security number (SSN), banking information, and/or PINs.
- It is good practice to change passwords on a regular basis, but Internet users should use strong passwords. For users with many complex passwords, another option is a password manager. **Do not** use the same password(s) for all of your accounts.
- Monitor financial records: check bank statements and credit card bills each month for odd charges.
- Keep your computer, devices, and software updated.
- **Do not** click on unknown links or attachments; these can launch malware on your computer and also have an impact on your contacts list. Don't forget the power of a phone conversation if you're unsure of the e-mail content.
- Know and recognize safe and reputable websites. If you're unsure of a website address, use a search engine to alleviate the risk of an unintentional visit to a similar but very different website. Verify the padlock sign is locked on secure sites before entering personal information.

So, would you fall for a scam? As IT experts on campus, we need to set a good example of how to stay safe online, which includes keeping up with changing technology and evolving cybercrime trends. Let's leave the thrillers on the big screen.

Note

1. For additional resources about staying safe online, visit the National Cyber Security Alliance website.

Marcia L. Dority Baker is the assistant director for academic technologies in Information Technology Services (ITS) at the University of Nebraska–Lincoln.