Internet Safety

Avoiding Hoaxes, Scams, and Other Icky Stuff

The Internet is a very powerful tool that has completely changed how we research, communicate, and interact with one another. Like anything else so powerful, the Internet is not without its risks and dangers. While the Internet should definitely be respected, you don't need to be afraid of it. With the proper knowledge, critical thinking, and risk awareness, you can stay safe on the Web.

The Dark Side of the Web

The Internet is generally a normal, mundane place that runs smoothly. Every so often, though, a user will find himself or herself on the dark side of the Web. This is the place where most problems arise. It is where many inexperienced users run into trouble. On the surface, the dark side of the Web can be hard to identify, but it usually appears in one of these three forms:

- Hoaxes
- Phishing scams
- Malware

Sometimes, the results of falling prey to these dangers are relatively harmless. At other times, they can lead to more serious problems like identity theft and computer damage. In any case, it's best to avoid them as much as possible.

Hoaxes

You know that scary "news" story that's going around on Facebook? That forwarded email about the New World Order? That secret trick about weight loss that "doctors don't want you to know about"? It's likely that you've seen a few of these in your time on the Internet. It's equally likely that when you *do* see things like this, they are not true but are instead cleverly disguised deceptions known as **hoaxes**.

How to identify hoaxes

Hoaxes can sometimes look very legitimate and realistic, so they aren't always easy to spot. Most hoaxes, however, will have certain characteristics:

- **"Shock value."** They use shocking headlines and words to lure people into reading.
- **Moral panic** or **appeals to fear**. They play on people's fears and uncertainties, contriving shady conspiracies and hidden agendas where none can legitimately be found.
- **Anecdotal ("he-said/she-said") evidence**. They don't support their claims with anything but eyewitness accounts, the most unreliable form of evidence.
- **Number spam**. They include a barrage of statistics – most of which are misrepresented or just made up – to prove their claim.

- **Claims of hidden or insider knowledge**. They include catch-phrases like "the government doesn't want you to know this" or "why isn't the mainstream media reporting this?" in an effort to make readers think they are getting some kind of hidden knowledge.

What you can do about hoaxes

The best way to avoid hoaxes is to be skeptical about *everything*. Take a guilty-until-proven-innocent approach. If you see something outrageous (or even not so outrageous) on Facebook, email, or other Web sites, *assume it's a hoax* until you find the information in reliable sources.

Research is an excellent tool for combating hoaxes. If you see a shocking story, try to find more information about it in legitimate, recognized sources. There are some sites, like Snopes, Politifact, and Factchecker, that are specifically devoted to sniffing out and debunking hoaxes.

Most importantly, if you find a hoax, don't make yourself part of the problem by spreading it. Most hoaxes are fairly harmless, but they are still based on deception and manipulation. Do the research *before* you share that Facebook post or forward that email.

Phishing Scams

People often think that scams are the same thing as hoaxes. In many ways, they are similar, but there are some key differences. While phishing scams and hoaxes are both based on manipulation, appeals to emotion, and scare tactics, **phishing scams** have the specific purpose of getting personal information from a user.

How to identify phishing scams

Phishing scams can take many forms, but they most commonly appear as emails. Facebook is generally good about keeping phishing scams off the site, but they do sometimes appear there, too, so it's always good to be cautious. Scams exhibit many of the same characteristics as those of hoaxes, but they may also have these traits:

- **Tragic backstories**. Phishing emails often appear to be written by a stranger with a terminal disease who wants to start a charity with her fortune, or a wealthy foreign banker who needs a business partner.
- **"Loud" text**. They often use ALL CAPS and exclamation points (!!!).
- **Bad spelling and grammar**. They are full of spelling errors and problems with sentence structure, and they appear to be written by someone who is not fluent in English.
- **Threats**. They claim that one of your online accounts has been compromised and threaten to cancel or block your account if you don't give them information.
- **Fake links**. They have links that are similar to Web sites of real companies or links that have been disguised as different links.

Phishing scams are usually much more dangerous than hoaxes because they are a direct attempt to get information from users.

What you can do about phishing scams

As with hoaxes, the best tool for dealing with scams is skepticism. If you assume most emails are phishing attempts (even if they are *not* in your junk mail folder), you are much less likely to get scammed.

If you get an email from a dying nun or a Nigerian businessman saying they have a huge sum of money they want to give you, *don't buy into it*. Scammers play on people's sympathies and emotions, and they do not mind lying to get what they want. In dealing with e-mails like this, there are two guiding principles that will keep you safe:

1. There's *no such thing* as free money.
2. If it *looks* too good to be true, it *is* too good to be true.

Pay close attention to the mechanics of an email. The more an email uses all caps and exclamation marks, the more suspicious you should be. Don't trust emails with bad spelling or grammar, *even if they look official*. Legitimate companies have people whose job is to check their publications for spelling and grammar, but scammers are known for bad grammar. If an email has bad grammar and spelling, it is far more likely to be from a scammer than an actual company.

Beware of *any* email that threatens you with account closures or tells you to "verify" your information (name, email, address, phone number, etc.) on an account you've made no changes to. Trustworthy companies *do not ask* for such information via email.

Do not click links in an email. It is very, *very* easy to disguise links, making you think you're going to one site when you're actually going to another. For example, hover your mouse over the following link, but don't click on it yet:

http://www.patrickhenry.edu/

This link *looks* harmless enough. It appears to simply be a link to the Patrick Henry Community College homepage. If you actually *click* on it, however, you'll be taken to a humorous page on Wikipedia instead of PHCC's Web site. This example isn't actually dangerous, but let's apply it to scammers. All it takes to make a fake link like the one above is a tiny snippet of code that *anyone* with even a basic knowledge of HTML can create. That means it's very easy for them to put a link to their own malicious site and disguise it as a link to Wells Fargo or Amazon.

When you're looking at an email, don't click links unless you're completely certain the email is actually from the company it appears to be from and isn't fake. If there is ever any doubt, call the company the email seems to be from (find their number online rather than using one in the email) and ask them about the email. If they don't know anything about it or if they say it is suspicious, leave it alone; it's probably a scam.

Malware

Another danger on the Internet is what it can put on your own computer. Sometimes, Web sites can contain malicious software, known as **malware**.

How to identify malware

"Malware" is a very broad term. Some malware is just annoying, but some can render a computer unsafe or unusable. It is usually downloaded from a Web site without a user's knowledge or consent. The term "malware" usually refers to one of the following (some of these categories can overlap):

- **Trojan horses**: Malicious software disguised as ordinary software (often used to steal a user's personal info, such as passwords, by recording what a user types and sending that information to the attacker).
- **Viruses**: Harmful software that installs itself on a computer and begins to replicate itself, usually destroying or corrupting files in the process.
- **Worms**: Similar to viruses. Worms can reproduce and take over an entire network of computers, allowing the attackers to use those computers for their own purposes (like sending spam emails or hosting illegal content).
- **Adware**: Software that floods a computer with unwanted advertisements (usually in the form of pop-up windows. It can also appear in the form of toolbars on a user's Internet browser).
- **Spyware**: Software that tracks a user or gathers information about a user without the user's knowledge.

Malware is often packaged together with legitimate software, so users often install it themselves without knowing it.

What you can do about malware

Malware can appear anywhere, but it does tend to be more common in some areas than in others. A good rule of thumb: if you go into a dark alley, don't be surprised if you get mugged. On the Internet, if you're trying to download bootleg software or going to pornography Web sites, you're much more likely to run into malware.

Malware is more likely to be found on shadier Web sites, but it can also appear in legitimate places. For this reason, it's good to have protection against malware. For Windows computers, Microsoft offers free virus protection called **Windows Defender** (it comes installed on Windows 8 computers; Windows 7 users can download the Windows 7 version, called Microsoft Security Essentials, for free on the Microsoft Web site). Another more heavy-duty antivirus called **Symantec** is available for free through the college (the download link can be found on Blackboard).

In addition to having a good antivirus, it's also important to always keep your software up to date. Most software companies occasionally make changes to their programs to make them safer and more difficult for hackers to tamper with. If you make sure you always have the latest version of the software, it will keep you more protected.

Because adware and spyware often comes bundled with legitimate software, always read the installation instructions very carefully. If possible, always choose the "custom" installation on software – it lest you see the list of things you're installing, and if you see something you don't want to install, you can uncheck that item.

Certain Internet browsers offer some additional protection against malware. For example, if you're using Google Chrome or Mozilla Firefox, you can install a site evaluator plug-in. The most common ones are Web of Trust and McAfee Siteadvisor. These programs look at Web links that appear in your browser (like on Google search results or Facebook posts) and rate them as safe or unsafe.

Sometimes, even if you're being as careful as possible, malware can still find its way onto your computer. If that happens, the important thing is not to panic. Malware can be scary, but keeping calm is the best way to recover your data. There is plenty of support available from people who constantly work to combat the threats of malware. There are also tools, like **Malwarebytes** and **Spybot Search & Destroy**, that are primarily designed to clean up infected computers. Prevention is the best medicine against malware, but the situation isn't hopeless, even if malware ends up on a computer.

Additional Writing Center Resources

- Using Sources

Further Reading

- Windows Defender: What it is and How it Protects You
  https://www.microsoft.com/security/pc-security/windows-defender.aspx
- Viruses, Worms, and Trojans – A Basic Guide to Malware
  http://huibit05.com/viruses-worms-and-trojans-a-basic-guide-to-malware/
- Snopes article: "6 Quick Ways to Identify Fake News"
  http://now.snopes.com/2015/04/28/six-ways-to-spot-fake-news/
- U.S. Securities and Exchange Commission resource on avoiding phishing scams
  http://www.sec.gov/investor/pubs/phishing.htm

Last update: 26 May 2015