



## Phishing Scams

by the School Internet Safety Initiative

**What is it?** Phishing scams usually include schemes that are meant to trick Internet users into sending money to one or more perpetrators (*online scammers*). Some examples include Internet auction fraud, where the seller may not send the buyer what they thought they had purchased; non-delivery of merchandise; and credit card, investment, and business fraud.<sup>1</sup> Identity theft is a form of an Internet scam where the perpetrator illegally obtains a victim's personal information to take up another person's identity. An estimate of 85 percent of all consumers have been deceived, defrauded, or cheated in some way from Internet scams, costing American consumers an average of over \$100 billion each year.<sup>2</sup>

**How is it done?** For phishing scams to succeed, victims must interact with a scammer online to some degree (e.g., through email or a chat room) and be tricked into sending or giving access to their money or online bank or credit card accounts. Tricking individuals into giving out their personal and financial information has become a profitable business for criminals, where they take advantage of the vulnerability of very trusting people.<sup>3</sup>

**What can you do to protect yourself?** When it comes to information on the Internet, both children and adults have the challenge of figuring out what content is truthful and what is not. Many people tend to trust the information they find online without questioning the source of the information. One of the best ways to avoid an Internet scam is to know what a phishing email/message or online fraud looks like in order to become better at judging online content and the accuracy of that information.

Know how to protect yourself from online scams<sup>4</sup>:


- Make sure a website address starts with 'https' (not just 'http') or look for a lock symbol in the search bar. This indicates that the site is more secure than a site without these symbols.
- Do NOT click on links in a suspicious email, even if you think you recognize the email address.
  - Hover your cursor over the questionable link in the email to see if it matches the *true link destination display*.
- Examine the email closely. If anything seems odd to you, this could be a phishing scam. Who sent it? What's the purpose? Is there anything unusual?
  - Does the message not make sense?
  - Are there spelling errors?

<sup>1</sup> Federal Bureau of Investigation. (n.d.). *Common fraud schemes: Internet fraud*. Retrieved from [https://www.fbi.gov/scams-safety/fraud/internet\\_fraud](https://www.fbi.gov/scams-safety/fraud/internet_fraud)

<sup>2</sup> Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing, 18*(7), 763–783.

<sup>3</sup> McNealy, J. E. (2008). Angling for phishers: Legislative responses to deceptive e-mail. *Communication Law & Policy, 13*(2), 275–300. doi: 10.1080/10811680801941292

<sup>4</sup> University of Houston. (2014). *Current phishing scams reported at UH*. Retrieved from <http://www.uh.edu/infotech/security/securedata/spamphishing/>

- 
- Does a company logo look different?
  - Does the sender make urgent requests, like asking you to send money or information immediately?
  - Beware of messages that claim your account has been suspended.
  - Be suspicious of any email containing urgent requests for personal or financial information.
  - Do NOT enter personal information in a pop-up screen.
  - Do NOT share your login and passwords with anyone you do not trust.
  - Do NOT give out personal or banking information over the Internet—banks do not usually ask for these things online.
  - Ask a trusted person, like a parent or friend for help if you need it, or see what others think of the email before you act.
  - Use the latest versions of your operating system (OS) and applications.
  - Have the latest security software updates installed, including patches for your OS and applications.
  - Keep your antivirus software up-to-date.
  - Report any suspicious emails to your teacher, parent, or an official group online, like the Federal Trade Commission at <https://www.ftc.gov/complaint>.

**For more information and to learn how to protect yourself from online scams, check out these suggested readings and resources:**

- Common Sense Education: *Scams and Schemes* <https://www.common sense media.org/educators/lesson/scams-and-schemes-6-8>
- Federal Bureau of Investigation: *Common Fraud Schemes* <https://www.fbi.gov/scams-and-safety>
- USA.gov: *Online Safety* <https://usagov.ctacdev.com/online-safety>
- Office of the Children’s Safety Commissioner (Australian Gov.): *Protecting Personal Information* <https://www.esafety.gov.au/esafety-information/esafety-issues/protecting-personal-information>