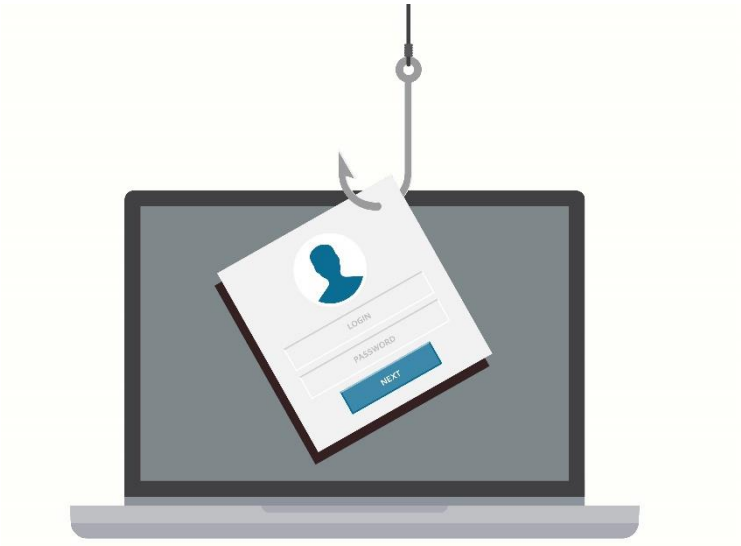
THE FACTS: BAITING

What is "baiting?"

Baiting involves leaving a piece of portable storage media such as a CD, laptop or USB stick in an open location to tempt a victim into seeing what's on it. When the victim opens files opens on the media, executes a malware program that releases a virus or leads to personal and financial information being exposed to hackers. If the victim uses a network, the infection can spread throughout the network.

Because flash drives are rarely encrypted, the files on them are easily accessed. One study that looked at 50 USB drives found not one was encrypted, and none of the files on them were password protected.



Baiting is similar to phishing, but unlike other types of social engineering it promises an item or goods to entice victims. For example, baiters may offer free music or movie downloads if the victim shares personal information such as login data and passwords. Baiting may also take place online, when cyber criminals post tempting offers or ads lead to malicious websites or get users to download malware-infected applications.

A 2016 report found that baiting is pretty successful. In one study 297 USB drives were dropped around the University of Illinois campus. Researchers verified that 45 percent were plugged into a device, but that 98 percent had been moved, so the number plugged in could have been much higher. The very first one dropped was found to be in use just six minutes later. In another study, 20 percent of 200 "finders" plugged in a drive found in public and opened files, clicked links or sent messages to an email address on the drive. Just 16 percent scanned the drive with antivirus software prior to use.

As of 13 June 2022

How do I protect myself from baiting?
Never plug an unknown piece of media into your computer. If you find a piece of media at your workplace, turn into your security officer. If you find it in public, it may be best to dispose of it. The best way to protect yourself is to not open any files on media you find. But if you do, make sure your security software is up to date and scan all files before attempting to open them.

For more on baiting and other forms of online social engineering, go to
https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

Follow ARCYBER on
(click the images to visit our pages)

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information dimension, while denying the same to our adversaries.

As of 13 June 2022