



# FACT SHEET

U.S. Army Cyber Command and Second Army  
The Nation's Army in Cyberspace  
www.arcyber.army.mil

---

## THE FACTS: PHISHING AND SPEARPHISHING

### ***What is "phishing?"***

Email attack is the preferred method for many hackers. Verizon's 2013 Data Breach Investigations Report found that "more than 95% of all attacks tied to state-affiliated espionage employed phishing as a means of establishing a foothold in their intended victims' systems."

In a phishing scam, a cybercriminal sends an email that attempts to fraudulently acquire the recipient's personal information. A phishing email might include an attachment or a link or request personal information. The email may appear to be a legitimate communication from your bank, phone company, a store you frequent, or a friend or coworker. A phishing email calls for an action, such as clicking on an embedded link, opening an attachment, or providing personal information.

### ***What is "spearphishing?"***

The higher up you are in an organization, the more likely you are to be a target for spearphishing -- specialized attacks against specific targets or small groups of targets to collect information or gain access to systems. In a spearphishing campaign, hackers have done their homework and learned the names of the target's subordinates, business associates, friends and perhaps even the clubs the target belongs to or the schools the target's children attend. Spearphishing emails typically appear to be from or about those close relations, and you don't have to be a senior executive to find mass-emailed phishing messages in your inbox.

Hackers run phishing campaigns because they work. Based on data collected by ThreatSim, Verizon calculated that "running a campaign with just three phishing emails gives a hacker a better than 50 percent chance of harvesting a click. At six emails, the probability goes to 80 percent, and with 10 emails, it's almost 100 percent certain that a target will have clicked and let a malicious payload into a targeted computer."

Additionally, on some sites that hackers love -- social media and banking websites -- emails are used as usernames. A hacker who knows his target's email address would then know their likely username for some accounts and could then try to crack the target's passwords on those accounts.

### ***What can I do to help avoid becoming a victim of phishing and spearphishing?***

**Call before you click.** Suppose you have an email that seems to be from your organization's human resources department telling you to complete an attached form to "update your personnel file." The attachment could be an executable malware file, or it could be a legitimate personnel update. Fight the natural instinct to trust an official-looking communication.

**ABOUT US:** Army Cyber Command and Second Army directs and conducts cyberspace and information operations as authorized or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries.

As of 3 September 2015

**Assume it's malware until proven otherwise.** Again -- call before you click. For example, ask HR whether they sent that email and why there was no other announcement about it, or call the number on the back of your bank card if you received an email threatening to close your account.

**When in doubt, throw it out.** Links in email, social media posts and online advertising are often the ways cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it or, if appropriate, mark it as junk email.

**Consider using specialized email accounts** – one for work, one for friends and one for online purchases. If you create a unique email address just for online payments, for example, it will be harder for a hacker to gain access to your information and account.

**Take advantage of free antivirus software and security checkups.** For a list of free security checks for your computer, visit <http://www.staysafeonline.org/stay-safe-online/free-security-check-ups/>.

Government employees can also get free antivirus software for home use at

[https://www.acert.1stiocmd.army.mil/Antivirus/Home\\_Use.htm](https://www.acert.1stiocmd.army.mil/Antivirus/Home_Use.htm)

**If you are a victim of phishing, report it.** You can report phishing to the appropriate people within your organization, such as network administrators, who can be alert for any suspicious or unusual activity. If you believe your financial accounts may be compromised, contact your financial institution immediately and close the accounts. Watch for any unauthorized charges to your account. Additionally, consider reporting the attack to your local police department, and file a report with the [Federal Trade Commission](#), the FBI's [Internet Crime Complaint Center](#) and/or the [Anti-Phishing Working Group](#).

For more, visit <http://www.staysafeonline.org/stay-safe-online>