

# The Front Burner Cyber Security



Office of the Chief Information Officer  
Office of Cyber Security

Issue No. 6  
November 2008

## *Social Engineering Works because Humans are the Weakest Link*

Social Engineering is a term for deceiving people into revealing confidential information. In most cases, hackers try to gain the confidence of an employee who has access to the required information. If done correctly, the employee does not even know that they have been conned, and the hacker can travel across our network undetected using "legitimate" credentials.

Security is all about trust. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found. It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.



### **Why would someone do this?**

The basic goals of social engineering are the same as hacking in general - to gain unauthorized access to systems or information in order to commit:

- Fraud
- Identity Theft
- Network Intrusion and Disruption
- Industrial Espionage

Social engineering attacks have two aspects: the physical (the location, such as in the workplace, over the phone, in the trash, online) and the psychological (the way it is carried out, such as persuasion, impersonation, ingratiation, conformity, and friendliness).

### **How might I be approached for information?**

Technical Support Personnel – An attacker pretending to be part of the technical support team

Important User - A hacker impersonating a senior manager

Helpless User - A hacker pretending to be confused and befuddled

### **Can I avoid being taken in by social engineering?**

There are several signs of social engineering attacks to recognize: refusal to give contact information, rushing, name-dropping, intimidation, small mistakes (misspellings, misnomers, odd questions), and requesting forbidden information. Try to think like a hacker and look for things that don't quite add up.

- Do NOT give out your password to anyone.
- Do NOT mention names of other employees or provide information about your organization or the Department unless you have verified the requester and the need to know.
- Use only thumbdrives and CDs you have received from reliable sources.
- Be wary of e-mails you aren't expecting, even when they appear to come from a reliable source. If you have any doubts, don't respond; call the HelpDesk for assistance.
- Do NOT click on Internet addresses in e-mails.

If you believe someone is using social engineering tactics to get information, notify your manager immediately.

**1. Know who you're dealing with.**

Check out unfamiliar sellers with the [Better Business Bureau](#) or state or local consumer protection agency. If you're buying gifts on an online auction site, check the track record of the seller before you bid. Don't buy from unsolicited emails from unknown companies.

**2. Get all the details.**

Get the name and physical address of the seller; how much the product or service costs; whether there are shipping charges; the delivery time, if any; the seller's privacy policy; and the cancellation and return policy.

**3. Look for signs that online purchases are secure.**

When you enter your payment information, the Web site address should change from http to shttp or https, indicating that the information is being encrypted — turned into code that can only be read by the seller. Some sellers also display banners or a lock and key pictures that indicate that the transaction is secured.

**4. Pay the safest way.**

Use a credit card. Under Federal law you can dispute the charges if you don't get what you were promised, and you have dispute rights if there are unauthorized charges on your credit card.

**5. Never enter your personal information in a pop-up screen.**

Legitimate companies don't ask for personal information via pop-up screens. Install pop-up blocking software.

**6. Keep documentation of your order.**

When you've completed the online order process, there may be a final confirmation page and/or you might receive confirmation by email. Print that information and keep it handy in case you need it later.

**7. Know your rights.**

Federal law requires orders made by mail, phone or online to be shipped by the date promised or, if no delivery time was stated, within 30 days. If the goods aren't shipped on time, you can cancel and demand a refund.

**8. Be suspicious if someone contacts you unexpectedly and asks for your personal information.**

Identity thieves send out bogus emails concerning consumer's accounts to lure them into providing personal information.

**9. Check your credit card and bank statements carefully.**

Notify the bank or credit card company immediately if there are unauthorized charges or debits, if you were billed incorrectly or there are any other problems.

**10. Keep your computer secure for safe shopping and other online activities.**

Protect your computer with spam filters, anti-virus and anti-spyware software, and a firewall, and keep them up to date. Go to [www.staysafeonline.org](http://www.staysafeonline.org) and [www.onguardonline.gov](http://www.onguardonline.gov) to learn more about how to keep your computer secure.

**11. Beware of emails offering loans or credit, even if you have credit problems.**

Con artists take advantage of cash-strapped consumers during the holidays to offer personal loans or credit cards for a fee upfront.

**12. Contact the seller promptly about any problems with your order.**

Check the company's Web site for a customer service page, "contact us" link, email address, or phone number. Do not click on links in e-mails unless you know it is legitimate.



## Ask Cyber Hero!

*Cyber Hero answers your security questions.*

Q: What's the best way to protect my DOE computer from an attack?

A: Don't click on what you don't know! If you aren't sure of the source or the sender, don't click on "OK" or open an attachment. Using "Alt-F4" will close a window (like a pop-up) even if it doesn't have a "Cancel" or "Close" option.

on the Web: <http://cio.energy.gov/cybersecurity.htm>  
by phone: 202-586-1090  
through e-mail: [cyber.security@hq.doe.gov](mailto:cyber.security@hq.doe.gov)