In A Nutshell…

Social Engineering & Information Security

What is social engineering?

Social engineering is the method of gaining access to information, data, physical work settings, and systems by exploiting human psychology, rather than by physically breaking in or using technical hacking techniques. It is a method of "human hacking".

What are the different types of social engineering?

Some of the most common types of social engineering attacks include:

- ☑ Phishing. This type of attack uses techniques to fraudulently obtain private information. This can be done via email, telephone, or other means.

- ☑ Dumpster Diving. As the term implies, this technique involves collecting information through organizations' dumpsters, including phone directories, memos, letterhead, disks, outdated hardware, etc.

> ***Students' Information Found In Dumpster***
>
> *Hundreds of Pittsburgh Public School Records with personal information about students were dumped on the side of the road. Dumpsters outside of a school were filled with report cards and behavioral reports, as well as names, addresses, phone numbers, and social security numbers of students.*
>
> *Source: pittsburgh.cbslocal.com, 06/21/11*

- ☑ Persuasion. Basic methods of persuasion include impersonation, conformity (convincing the individual that "everyone else is doing it"), and simple friendliness.

- ☑ Baiting. Sometimes compared to a "Trojan Horse", this technique uses media devices (e.g., infected USB flash drives, disks, etc.) and relies on the curiosity or greed of an individual to pick-up and use the infected media device.

- ☑ Tailgating. Sometimes referred to as "piggybacking", this technique involves the hacker seeking entry to a restricted area of an office or other location. In this case, the hacker may follow a legitimate individual into the secure area.

What can I do to prevent social engineering attacks?

- ☑ Be wary of phone calls, email, etc. from anyone asking for personal or confidential information. Do not release such information unless you are certain the request is legitimate.

- ☑ Do not provide any personal information or other information about your office/organization unless you are sure the person is authorized to have such information. When in doubt, verify the person's identity directly with their company.

- ☑ Do not send sensitive information via email or over the internet. If no other options for sending the information are available, make sure the information is secured and encrypted.

- ☑ Make sure that documents, electronic devices, etc. containing confidential information are properly destroyed when no longer needed.

- ☑ Be aware of your surroundings and report any suspicious or unauthorized people who may be wandering near secure areas. If the person claims to have legitimate business there, ask for identification or directly confirm it with their company.

What do I do if I'm hacked or if there's a security breach?

- ☑ Report attacks and breaches to the appropriate person(s) or office(s). Most organizations, including HIDOE, have guidelines and other documents to help guide you through the process of reporting a breach.

- ☑ If you receive any suspicious email or suspect an email is a phishing attempt, report it to the appropriate person(s) or office(s). Many email vendors have a way to report and/or block phishing or fraudulent email message.

- ☑ If the hack or breach occurred on a password-protected system, account, database, etc. change your password immediately. If the password is used for other accounts, etc., make sure to change those as well. Do not reuse the password in the future.

Where can I get more information?

Privacy Technical Assistance Center (PTAC)	
PTAC provides resources to educational stakeholders as it relates to data privacy, confidentiality, and security. The website contains technical briefs, white papers, archived webinars and presentations, and checklists.	http://ptac.ed.gov/
United States Computer Emergency Readiness Team (US-CERT)	
US-CERT is part of the Department of Homeland Security and leads efforts to improve cyber security, coordinate cyber information, and manage cyber risks. The site contains security publications and other resources, as well as alerts and tips.	http://www.us-cert.gov/
HIDOE FERPA & Student Privacy Website	
This website contains information about FERPA and other student privacy regulations, as well as department-specific information and forms.	Public content http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/StudentPrivacy/Pages/home.aspx Employee-related content https://intranet.hawaiipublicschools.org/offices/dgo/pse/Pages/default.aspx
HIDOE Security Breach Guidelines	
Guidelines to provide awareness of potential unauthorized access to personal information, as well as to provide instruction on how to take action to report incidents related to unauthorized access. These guidelines are consistent with Hawaii Revised Statutes HRS Chapter 487N – Security Breach of Personal Information.	https://intranet.hawaiipublicschools.org/offices/dgo/pse/Pages/default.aspx

Hawaii State Department of Education ◆ Data Governance Office
P.O. Box 2360 ◆ Honolulu, HI 96804
P: 808.218.6791 ◆ F: 808.440.2859
E: DGO@notes.k12.hi.us

Data Governance Office Websites
Public content
http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/HawaiiDataSources/Pages/Data-Governance.aspx

Employee-related content
https://intranet.hawaiipublicschools.org/offices/dgo