Information Security Awareness Cheat Sheet

by George_ITO via cheatography.com/36063/cs/11346/

Introduction - Information Security

Computer-related crimes affecting businesses or consumers are frequently in the news. While companies normally have technical defense systems in place, end-users and staff members also need to know how to protect and maintain their computer systems so they can steer clear of fraudsters. Here is a short set of recommendations for keeping yourself safe online.

Private data and its value

Protect your and your client's data

Hackers find private data very valuable. It is important that you protect ALL types of data as these can be used for many purposes, such as

- Identity theft
- Targeted attacks
- Data sold to other parties for data mining

Data such as personal information and system credentials are very sought after and will fetch a hacker a good price. Be always aware and always protect the information you handle.

Phishing

Phishing is one of the most common methods of attack nowadays. Phishing involves tricking a user into giving their password into a seemingly legitimate site. Use the list of tips below to increase your awareness and prevent your credentials from being stolen:

Be wary of emails asking for confidential information

Especially information of a financial or personal nature. Legitimate organizations will never request sensitive information via email, and most banks in NZ will tell you that they won't ask for your information unless you're the one contacting them.

Don't get pressured into providing sensitive information.

Phishers like to use scare tactics, and may threaten to disable an account or delay services until you update certain information. Be sure to contact the merchant directly to confirm the authenticity of their request.

Watch out for generic-looking requests for information.

Phishing emails are often not personalized, while authentic emails from your bank often reference an account you have with them. Many phishing emails begin with "Dear Sir/Madam", and some come from a bank with which you don't even have an account with.

Never submit confidential information via forms embedded within email messages.

Senders are often able to track all information entered into a form. If you suspect you may have entered information into an illegitimate form, proceed to change your passwords ASAP.

Never use links in an email to connect to a website unless you are absolutely sure they are authentic.

Instead, open a new browser window and type the URL directly into the address bar. Often a phishing website will look identical to the original - look at the address bar to make sure that this is the case.

Other types of attacks

Be aware of other types of attacks you may encounter

Smishing

SMS Phishing is called smishing, and it is a form of social engineering technique that attempts to acquire personal information (such as your password) by masquerading as a trustworthy company via text messages on your mobile phone. If you receive an unsolicited, seemingly legitimate SMS text from a bank, service or company, don't open the accompanying link. Instead, call them directly in regards to the text message contents if required.

Vishing

Vishing is the telephone equivalent of phishing. It is often an attempt of acquiring information using the telephone. Oftentimes these are calls from IRD, Microsoft or other service providers with an apparently legitimate query for further information. Be wary and if in doubt always hang up and call their known, main number instead.

Best Practices

Be careful where and how you connect to the Internet.

A public computer, such as at an Internet café or hotel business center, may not have up-to-date security software and could be infected with malware. Also, for online banking or shopping, avoid connecting your computer, tablet or smartphone to a wireless network at a public "hotspot" (such as a coffee shop, hotel or airport).

Be suspicious of unsolicited e-mails and text messages asking you to click on a link or download an attachment.

It's easy for fraudsters to copy corporate or government logos into fake e-mails that can install malware on your computer.

Your best bet is to ignore any unsolicited request for immediate action or personal information, no matter how genuine it looks. If you decide to validate the request by contacting the party that it is supposedly from, use a phone number or e-mail address that you have used before or otherwise know to be correct. Don't rely on the one provided in the e-mail.

Use "strong" IDs and passwords and keep them secret.

Choose combinations of upper- and lower-case letters, numbers and symbols that are hard for a hacker to guess. Don't, for example, use your birth date or address. Also don't use the same password for different accounts because a criminal who obtains one password can log in to other accounts. Finally, make sure to change your passwords on a regular basis.

Data leaks

Preventing data leaks is something everyone can do. Follow these recommendations to ensure that you are not unknowingly disposing of private data that could end in the wrong hands:

1. Always shred or destroy private information you no longer need
2. Do not take USB pendrives with confidential data out of the office if possible
3. Use encrypted USB drives for data you need to take out of the office
4. Always securely dispose of devices (computers, laptops and cellphones) to avoid data being leaked by accident.

By **George_ITO**
cheatography.com/george-ito/

Not published yet.
Last updated 13th April, 2017.