Cybersecurity Red Flags Cheat Sheet

by [deleted] via cheatography.com/2754/cs/9888/

Introduction

For years, hacking focused mainly on stealing computing resources to create for example, botnets. Today, the focus has shifted to stealing the most valuable thing the users have – their personal data. Personal data ranges from names and addresses, to logins and passwords, credit card numbers, Social Security numbers and information about where an individual is located and what they are doing. Access to this information not only leads to identity scams but can also jeopardize an individual’s personal safety as well. In order to build a solid cybersecurity system and combat attacks it is important for users to understand common cyber-threats.

Credits: http://www.securitymagazine.com/articles/85679-special-report-cyber-risk-and-security - Larry Bridwell

Phishing

Phishing attacks appear in two forms, targeting a large number of individuals or focusing on a specific group. Mass attacks aim to deliver malware via automatic download to users’ devices and often come in the form of USB flash drives or infected websites and emails. Targeted attacks come in the form of tailored emails that are disguised as emails from large corporations. Targeted phishing emails often include corrupted links and ask for personal information or automatic actions.

Social networks

Posts or links to websites that offer an option to sign up through your social network accounts with the click of a button provides hackers with access to your list of friends and your personal information. What is worse, some malware can be downloaded onto your device without the user’s knowledge. The delivery can take place immediately or with some delay so the victim cannot easily track down the source of the malware.

Infected websites

Some websites can contain malware that utilizes the security holes in browsers. It is impossible for the user to be aware of all possible threats and without the proper security software, and up-to-date operating system and browsers, people are under constant threat.

Public Wi-Fi Networks

Accessing public Wi-Fi networks leaves individuals vulnerable to hackers as these networks can easily be monitored to obtain private information. By not using an encrypted website when accessing sensitive data, people are simply leaving the door open to hackers.

User Service Providers

When creating an account, users provide their personal information with good faith in their security. Attacks similar to the Target hack and Heartbleed exemplify a hacker’s option to target third-party maintenance organizations to gain access to users’ personal data.

Tips

- Use strong passwords; mix numbers, upper and lower case letters and symbols
- Use unique passwords for each site you use or utilize a password management system that can do it for you
- Keep your operating system, security software, browsers etc. up to date
- Be careful when asked to click links that you receive in email or social media messages
- Treat everything you post as if it will be completely public and never be deleted – everything
- Status updates, photos and comments can reveal A LOT about you
- On social networks be selective about who you accept as a friend, and be careful about adding apps, plugins or other extras
- Always enable the **passcode lock** on your phone and mobile devices