Lab – Discover Your Own Risky Online Behavior

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

a. What kind of information do you share with social media sites?

1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
2) Articles and news I find or read (2 points)
3) It depends; I filter out what I share and with whom I share. (1 point)
4) Nothing; I do not use social media. (0 points)

b. When you create a new account in an online service, you:

1) Re-use the same password used in other services to make it easier to remember. (3 points)
2) Create a password that is as easy as possible so you can remember it. (3 points)
3) Create a very complex password and store it in a password manager service. (1 point)
4) Create a new password that is similar to, but different from, a password used in another service. (1 point)
5) Create an entirely new strong password. (0 points)

c. When you receive an email with links to other sites:

1) You do not click the link because you never follow links sent to you via email. (0 points)
2) You click the links because the email server has already scanned the email. (3 points)
3) You click all links if the email came from a person you know. (2 points)
4) You hover the mouse on links to verify the destination URL before clicking. (1 point)

d. A pop-up window is displayed as you visit a website. It states your computer is at risk and you should download and install a diagnostics program to make it safe:

1) You click, download, and install the program to keep your computer safe. (3 points)
2) You inspect the pop-up windows and hover over the link to verify its validity. (3 points)
3) Ignore the message, making sure you don't click it or download the program and close the website. (0 points)

e. When you need to log into your financial institution's website to perform a task, you:

1) Enter your login information immediately. (3 points)

2) You verify the URL to ensure it is the institution you were looking for before entering any information. (0 points)

3) You don't use online banking or any online financial services. (0 points)

f. You read about a program and decide to give it a try. You look around the Internet and find a trial version on an unknown site, you:

1) Promptly download and install the program. (3 points)

2) Search for more information about the program creator before downloading it. (1 points)

3) Do not download or install the program. (0 points)

g. You find a USB drive while walking to work. you:

1) Pick it up and plug it into your computer to look at its contents. (3 points)

2) Pick it up and plug it into your computer to completely erase its contents before re-using it. (3 points)

3) Pick it up and plug it into your computer to run an anti-virus scan before re-using it for your own files (3 points)

4) Don't pick it up. (0 points)

h. You need to connect to the Internet and you find an open Wi-Fi hotspot. You:

1) Connect to it and use the Internet. (3 points)

2) Don't connect to it and wait until you have a trusted connection. (0 points)

3) Connect to it and establishes a VPN to a trusted server before sending any information. (0 points)

Part 2: Analyze Your Online Behavior

The higher your score, the less safe your online behaviors are. The goal is to be 100% safe by paying attention to all your online interactions. This is very important as it only takes one mistake to compromise your computer and data.

Add up the points from Part 1. Record your score.

0: You are very safe online.

0 – 3: You are somewhat safe online but should still change your behavior to be completely safe.

3 – 17: You have unsafe behavior online and have a high risk of becoming compromised.

18 or more: You are very unsafe online and will be compromised.

Below are a few important online safety tips.

a. The more information you share on social media, the more you allow an attacker to know you. With more knowledge, an attacker can craft a much more targeted attack. For example, by sharing with the world you went to a car race, an attacker can craft a malicious email coming from the ticketing company responsible for the race event. Because you have just been to the event, the email seems more credible.

b. Reusing passwords is a bad practice. If you reuse a password in a service under attackers' control, they may be successful when attempting to log in as you in other services.

c. Emails can be easily forged to look legitimate. Forged emails often contain links to malicious sites or malware. As a general rule, do not click embedded links received via email.

d. Do not accept any unsolicited software, especially if it comes from a web page. It is extremely unlikely that a web page will have a legitimate software update for you. It is strongly recommended to close the browser and use the operating system tools to check for the updates.

e. Malicious web pages can be easily made to look like a bank or financial institution website. Before clicking the links or providing any information, double-check the URL to make sure it is the correct web page.

f. When you allow a program to run on your computer, you give it a lot of power. Choose wisely before allowing a program to run. Research to make sure the company or individual behind the program is a serious and legitimate author. Also, only download the program from the official website of the company or individual.

g. USB drives and thumb drives include a tiny controller to allow computers to communicate with it. It is possible to infect that controller and instruct it to install malicious software on the host computer. Because the malware is hosted in the USB controller itself and not in the data area, no amount of erasing or anti-virus scanning will detect the malware.

h. Attackers will often deploy fake Wi-Fi hotspots to lure users. Because the attacker has access to all the information exchanged via the compromised hotspot, users connected to that hotspot are at risk. Never use unknown Wi-Fi hot spots without encrypting your traffic through a VPN. Never provide sensitive data such as credit card numbers while using an unknown network (wired or wireless).

Reflection

After analyzing your online behavior, what changes would you make to protect yourself online?