Web Usage

What Is Safe Browsing and Why Is It Important?

The internet is full of hidden dangers.

Since we use the internet on a daily basis, it's important to practice safe browsing to ensure that you and the people you connect with stay safe.

Viruses

Viruses and other forms of malicious software – called malware – are able to infect computers by hiding within software that is available for download on the internet.

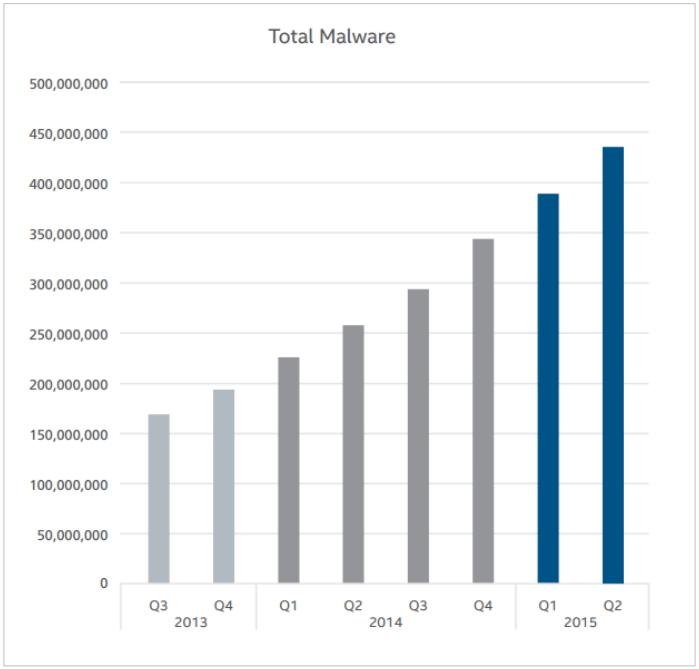
Social Engineering

Hackers often use social platforms, such as email and social media, to trick people into revealing their user names and passwords for various accounts.

Identity Theft

Your personal information is valuable to hackers. If they are able to obtain it, they could empty your bank accounts, sell it to other people, or hold it for ransom.

Over time, the amount of malware continues to increase:



Source: McAfee Labs Threats Report, August 2015

How Does It Affect You and Your Organization?

Malware acts like a human virus
and your computer is used to spread it around.

Unsafe browsing could make **you** sick!

- Your corporate computer is not impenetrable. Certain websites could deliver a virus to your computer.
- Hackers will use clickable links to download malware onto your computer. This malware could cause irreversible damage to the files on your computer.
- A compromised corporate computer can not only leak personal information to unauthorized users, but it can also cost the company a lot of money.

Unsafe browsing could make **others** sick!

- Malware can be passed between computers. Computers that are suspected to be infected should be reported to the IT department immediately.
- An infected computer connected to the internet can be used by a hacker to send fake messages to your contacts, Facebook friends, Instagram followers, etc. These messages will contain links that if clicked, download the malicious software onto their computers.

Avoid Getting Infected in the First Place

- The best way to avoid infecting other computers and keeping your own computer safe is to avoid getting infected with malware in the first place.
- Practicing the safe browsing habits discussed in this training module will help keep your computer safe from viruses.

Threat Identification

How can you tell if your computer has been compromised?

A Slow Computer

Sometimes, a slow computer means that your system has been infected. Malware tends to slow down your computer's operating system, making applications unusually slow.

A Crashing Computer

If you find that applications or your entire computer often crashes unexpectedly, it may be infected with malware.

Annoying Pop-ups

Getting unwanted pop-ups is a sign that your computer has been infected. Often the malware causing the pop-ups is doing further damage to your computer in the background.

Fake Email/Social Media Messages

If your friends/colleagues tell you that they have received messages from you that you didn't send, your computer is likely infected with malware and it is trying to infect other people.

Unexpected Software

If you notice software on your computer that was recently downloaded without your permission, it is likely a malicious program.

Disabled Antivirus Software

Certain types of malware will disable your antivirus software when your computer becomes infected.

Source: Andra Zaharia. "10 Warning Signs that Your Computer is Malware-Infected." Heimdal Security.

Be Proactive

AVOID …	INSTEAD …
Clicking on pop-up advertisements or intriguing graphics.	Please consult workstation support before installing any software.
Quickly clicking on links, even from sources that you trust.	Hover your mouse over the link to see the address that the link will be directing you to. If the address isn't what you expected, don't click on the link.
Visiting untrustworthy sites.	Ensure that the website you are visiting is secure by looking at the address bar. A secure website will have "https://" before the website address. If the "**s**" is missing and "http://" appears instead, the website may not be secure.
Doing personal things, like accessing email or bank accounts, while connected to insecure networks, such as public Wi-Fi.	Only use insecure networks as a last resort. Hackers may be monitoring the information sent over these networks, making them a dangerous place to input account information.

Be Proactive

Follow these practices to help protect you and your device:

- ✓ Use caution when surfing the web. If something looks suspicious, trust your instincts.
- ✓ Create strong passwords that are easy to remember. This is important, since allowing websites to autofill your account information puts your accounts at risk if somebody steals your device.
- ✓ Watch out for phishing emails – hackers will try to trick you into clicking links and providing personal information. Learn more about phishing to further protect yourself against these kinds of attacks.
- ✓ If you use online banking, regularly monitor your bank statements. Alerting your bank to unusual activity in your account could save you a lot of money.
- ✓ Always be mindful of the performance of your computer. If it is behaving in an unusual way, it may be infected with malware.
- ✓ **If you believe that your corporate computer has been infected, report it to Bruin Support Services at 1.800.756.7920**

Reporting and Contact Information

If you have any general questions:

– Bruin Support Services at 1.800.756.7920

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.