Reading 2

Skills:

- Details
- Author's attitude
- Vocabulary in context
- Understand negative facts

Getting started: What internet browser do you use? Why do you prefer that one?

ARE INSECURE DOWNLOADS INFILTRATING YOUR CHROME BROWSER?

The internet is quite a bit safer than it once was. Recent large-scale adoption of the HTTPS standard means that internet traffic is largely encrypted, providing a high standard of protection against hackers and attacks. In 2018, over 50 percent of websites used HTTPS protection for the first time ever. This number continues to grow, with 96 out of the 100 top non-Google sites defaulting to HTTPS, an amount that represents a quarter of all web traffic.

Unfortunately, HTTPS is not completely invulnerable. It encrypts your connection, but it doesn't inspect the encrypted traffic. This means that your (supposedly) secure connection is totally

capable of receiving malware and that phishing sites can easily fool people by displaying the secure lock icon to the left of their URL. Over half of phishing sites now use HTTPS, and a new study shows that almost 70 percent of malware was delivered via an HTTPS connection. Much of this malware delivery occurs via an HTTPS **loophole** known as a "mixed content download." In this type of attack, you visit a website that's secured with the familiar HTTPS lock symbol. If you download something from the site, however, it can come from an insecure address or even a secure address that happens to **host** malware. As a result, the content you download from the site has the potential to be infected with malware.

Mixed content downloads have evolved. If the mixed content download occurs via a developer error, then the download itself may not present that much of a risk. The major vulnerability is if a developer accidentally creates a resource for download that was contaminated by malware (such as an infected PDF), or if an attacker obtains developer credentials and does the same thing. Increasingly, attackers are building phishing sites that make use of the HTTPS standard and then implement mixed-resource downloads. As ordinary users may not know exactly what HTTPS does, they never suspect that a website that uses the lock symbol might still be trying to phish their credentials or infect their computer.

Google is clearly **aware** of the mixed content download problem, but it's arguably moving too slowly. In the Chrome 81 version (April 2020), Google added popup warnings to users if they initiated an insecure download on a secure site. An August 2020 version of Chrome blocked all downloads except images, audio, video, and text. By October 2020, mixed content downloads were blocked entirely. An extended timeline like that gives legitimate developers plenty of time to pull insecure download links and place them with secure ones, but it also gives bad actors plenty of time to act.

Attackers have many ways to turn malicious content into legitimate-seeming resources using Chrome. For example, Chrome extensions, which are software **applets** designed to extend the functionality of the browser, can often be used for harm. All extensions are promoted through the Chrome Web Store, which is supposed to automatically check extensions for malicious content. These extensions have conferred an air of legitimacy, in other words, but attackers use this legitimacy to cause problems. In June 2020, Google removed over 100 malicious extensions

that had been designed to fool security checks, take screenshots of the browser, monitor users' keystrokes, and more. Collectively, these extensions were downloaded by nearly 33 million people. This isn't an isolated incident. In 2019, 1.5 million people downloaded a pair of apps disguised as popular ad-blocking extensions. Instead of blocking ads, however, the applications loaded malicious tracking cookies onto users' systems. The year before that, a different Chrome extension was discovered to be part of a **botnet** that infected websites with **cryptojacking** code.

The point is that even though Chrome is advertised as being a secure mainstream browser (and that's not a false claim—it's definitely secure), security is relative. In some ways, Chrome's reputation for security works against it. Because users think that Chrome is secure, they often think that it's more secure than any browser could possibly be. Essentially, attackers are too clever for any browser to be truly secure, and no amount of security awareness training will teach every user to avoid phishing sites, especially when those phishing sites are secured by HTTPS, which makes them look extremely legitimate.

**Adapted from https://www.techopedia.com/are-insecure-downloads-infiltrating-your-chrome-browser/2/34384*

Glossary:

- **Loophole**: a loophole is an error or opening in the computer code allowing a program to be manipulated or exploited. This term generally comes up when referencing computer or network security.
- **Applet**: a program that is run from within another program, for example from within an internet browser.
- **Botnet**: Alternatively referred to as a zombie network, a botnet (bot network) is a group of infected computers that are under the control of one or more individuals. The infected computers perform tasks impossible for a single computer, such as distributing millions of SPAM e-mail's or a Distributed Denial of Service (DDoS) attack.
- **Cryptojacking**: Cryptojacking is the malicious use of a person or people's computing power to **mine cryptocurrencies** without consent.
- **Mine cryptocurrencies**: The practice of "cryptomining" or cryptocurrency mining involves adding various cryptocurrency transactions and evidence of mining work to the blockchain ledger. As a miner works to generate the block contents and algorithmic outputs that make up new

blockchain transactions, they are said to be creating a new "coin" of a particular kind in the blockchain.

Answer the following questions:

1. What's the author's attitude towards internet security?
    a. He/she thinks that even when security measures are developed, attackers will always find a way to take advantage of people.
    b. He/she is completely sure that Google Chrome is almost invulnerable and just a few attacks could take place in this browser.
    c. He/she is optimistic IT professionals will find a way to block any possible cyberattack in the near future.
    d. He/she believes Google provides the safest measures on the internet.

2. What is stated about HTTPS protection?
    a. Developers started using this kind of connection in 2018.
    b. 50% of Google sites use this type of protocol.
    c. HTTPS is susceptible to cyberattacks.
    d. Although it inspects traffic, it doesn't encrypt your connection.

3. A high percentage of the malware delivered through an HTTPS connection occurs due to
    a. unsecure connections
    b. a loophole
    c. public computers
    d. Google Chrome

4. The word **host** in paragraph 2 is closest in meaning to
    a. stay
    b. store
    c. organize
    d. introduce

5. What is NOT stated about mixed content downloads?
    a. Attackers create HTTPS sites with mixed content downloads to infect a computer.
    b. Even if a site has the lock symbol, it can store malicious mixed content.
    c. A developer can unconsciously upload mixed content downloads.
    d. It could be more serious if it happened because of a developer mistake.

6. The word **aware** in paragraph 4 is closest in meaning to
    a. conscious
    b. insensible
    c. expert

d. interested

7. How does the author seem to feel about Google Chrome in paragraph 4?
    a. He/she says Chrome often warns its users, that's why attacks are always prevented.
    b. He/she believes Google Chrome updates are nothing but useless.
    c. He/she thinks Google could act faster to prevent cyberattacks.
    d. He/she believes Chrome should always allow people to download music and pictures.

8. What is stated about Google Chrome extensions in paragraph 5?
    a. Ad-blocking extensions are necessary to control these apps.
    b. The applets are the most functional complements for the browser.
    c. Many of these extensions have been removed because they were dangerous.
    d. In 2019, 33 million people downloaded malicious extensions that infected their PCs.

What do you think?

Do you feel safe when you surf the internet?