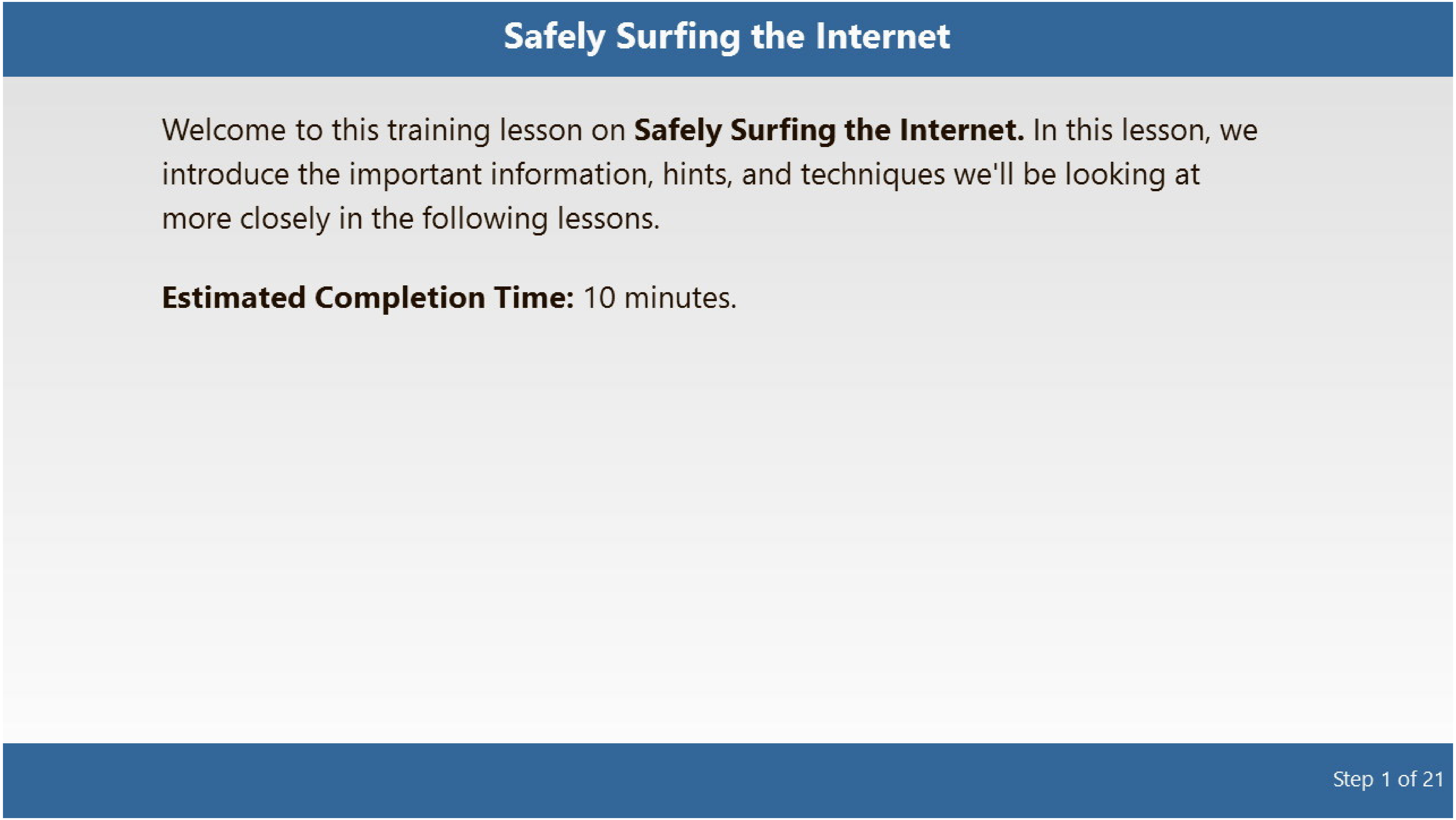


Safely Surfing the Internet

Welcome to this training lesson on **Safely Surfing the Internet.** In this lesson, we introduce the important information, hints, and techniques we'll be looking at more closely in the following lessons.

Estimated Completion Time: 10 minutes.

Safely Surfing the Internet

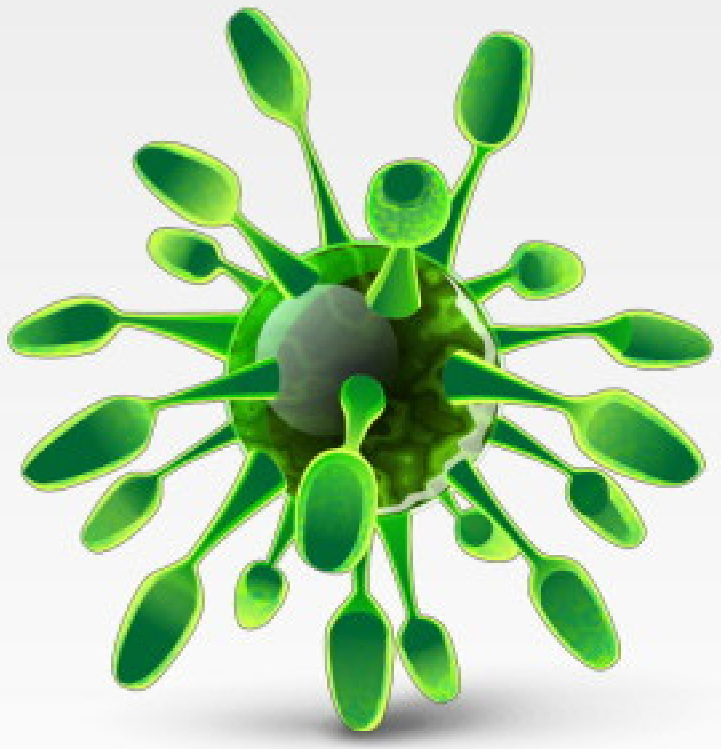
Introduction. In this lesson, we will be looking at general safety hints, tips, and techniques related to surfing the web.

In up and coming lessons, we look specifically at safety related to **Web Surfing, Viruses, Email, Social Media, Passwords, User Names, Purchasing Online** and many more.

Safely Surfing the Internet

Viruses. One of the main goals of safe web surfing is to avoid viruses. Viruses are unwanted, malicious software installed on your machine without your consent. They may mess with your machine, may perform operations in the background under someone elses control - and may even hold your data to ransom.

Viruses come in different shapes and forms. You'll variously hear certain types being referred to as *trojans (trojan horses)*, *spyware*, *adware*, *worms*, or *trackers*. Each is slightly different in the way they operate, but the bottom line is that you don't want any of them.



Safely Surfing the Internet

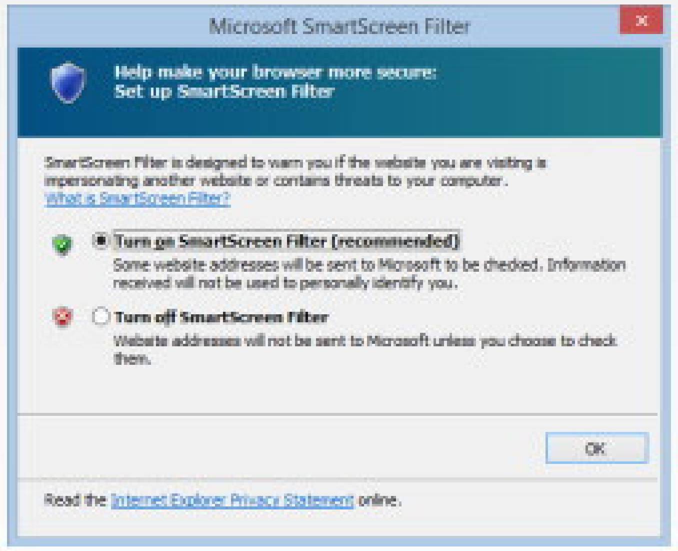
Antivirus Software. If you are using anti-virus, or security software (and you should!), many of these programs will automatically link to your Internet Browser to provide an extra level of security. They can detect dangerous attachments, dangerous sites, and other suspicious activity - and block them all.

Safely Surfing the Internet

Browser Safety Controls. Many Internet browsers - and in particular, Internet Explorer, have a range of security features you can enable to help protect you while web surfing. Many of these are complex, and a little hard to understand.

However, if you browser contains a feature like - as in Internet Explorer - called **SmartScreen Filter** - or perhaps, in other browsers, called something like **Phishing Control,** or **Malware control** (generally, these are enabled by default), it's a good idea to keep them on - or turn them on. They'll help protect against fraudulent and dangerous websites.

We cover this in much more detail in the **Browser Safety Options** lesson.



Microsoft SmartScreen Filter

Help make your browser more secure:
Set up SmartScreen Filter

SmartScreen Filter is designed to warn you if the website you are visiting is impersonating another website or contains threats to your computer.
What is SmartScreen Filter?

● **Turn on SmartScreen Filter (recommended)**
Some website addresses will be sent to Microsoft to be checked. Information received will not be used to personally identify you.

○ **Turn off SmartScreen Filter**
Website addresses will not be sent to Microsoft unless you choose to check them.

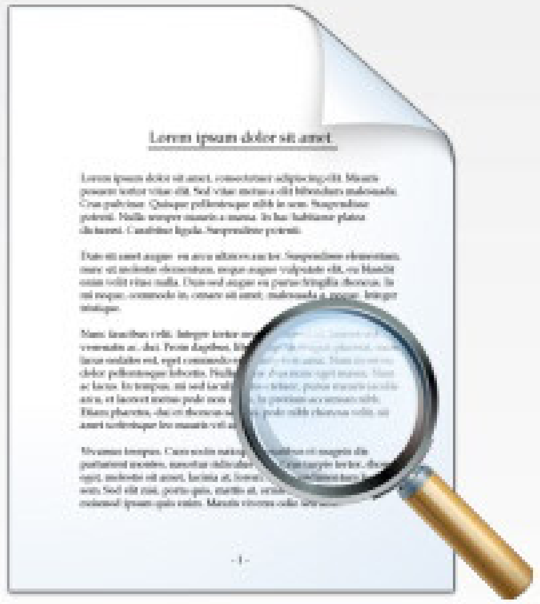
Read the Internet Explorer Privacy Statement online.

Safely Surfing the Internet

Secure Your Information. Many websites will ask you for your details to subscribe to a newsletter, receive a special offer, receive email updates, or a dozen other reasons.

Most sites - and certainly most reputable sites - will have, by law, a privacy policy. This is normally a link on most pages in the site, and will outline what they can do with your private information. For example, whether they sell or share email addresses with other clients.

Before you give any information - even something as simple as an email address, read the privacy policy. If you don't like what you read, don't provide any information.



Safely Surfing the Internet

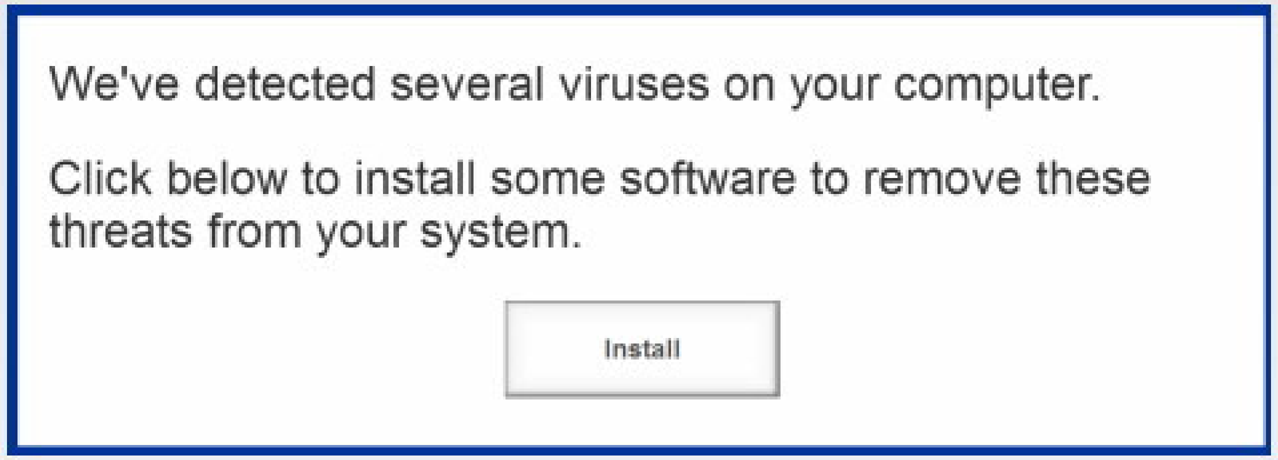
Downloads. Be very careful with what you download from websites. This especially refers to such things as games. Quite often, along with the game, you'll get a virus, trojan, or some other malicious software installed on your computer. Sometimes these are just annoying, and sometimes they are dangerous.

If you have anti-virus software - and again, you should - ensure that any software you download is scanned by the anti-virus software before and after it is installed.

Only download software from reputable sites.

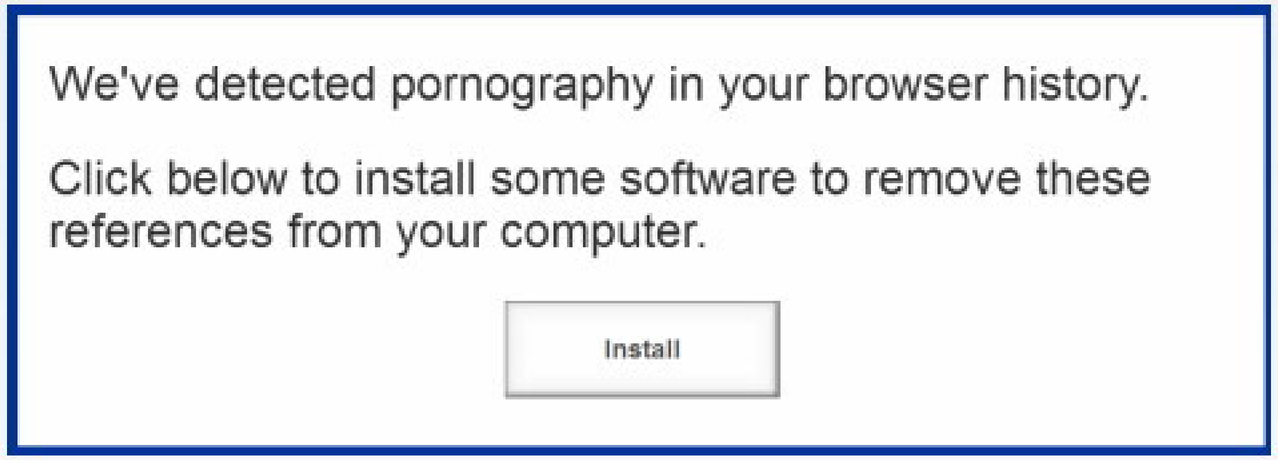
Safely Surfing the Internet

Don't Fall For It. Hackers and scammers will do anything to get you to install some software. Some of the methods seem very realistic. For example, you may see something like this while surfing the web:



We've detected several viruses on your computer.

Click below to install some software to remove these threats from your system.



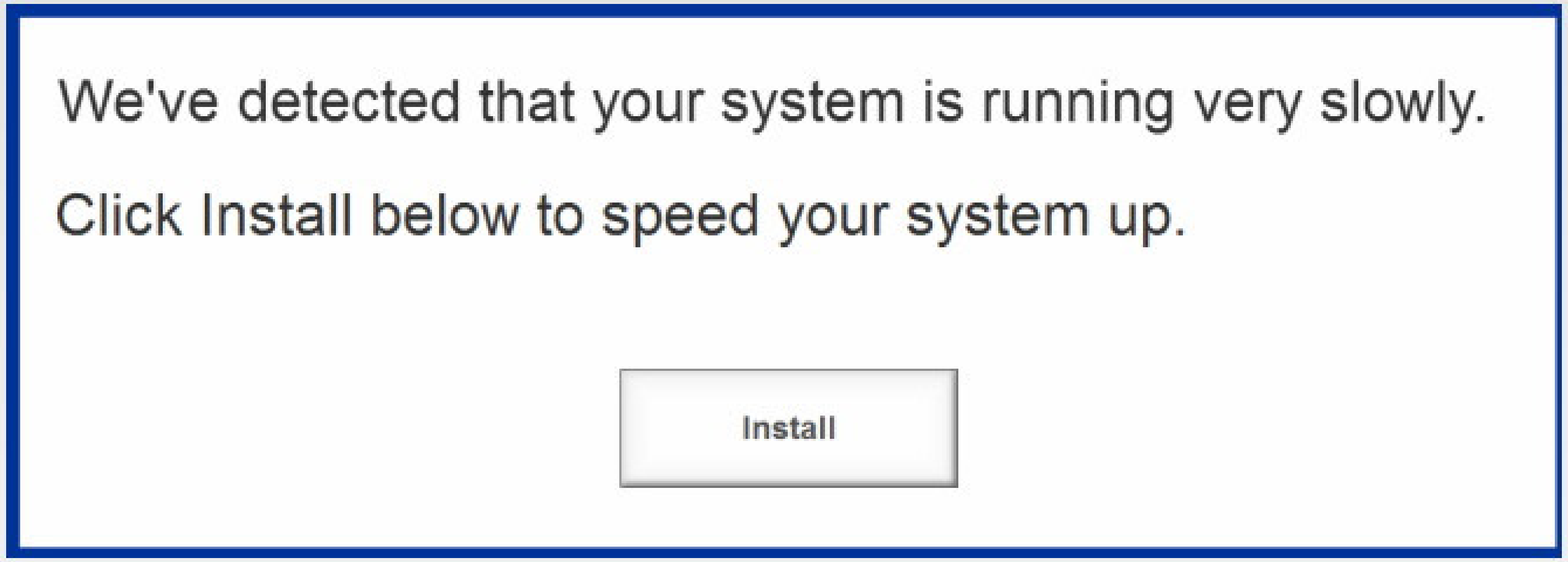
We've detected pornography in your browser history.

Click below to install some software to remove these references from your computer.

Such messages are **always** scams. **Never install** software from websites that display messages anything like this.

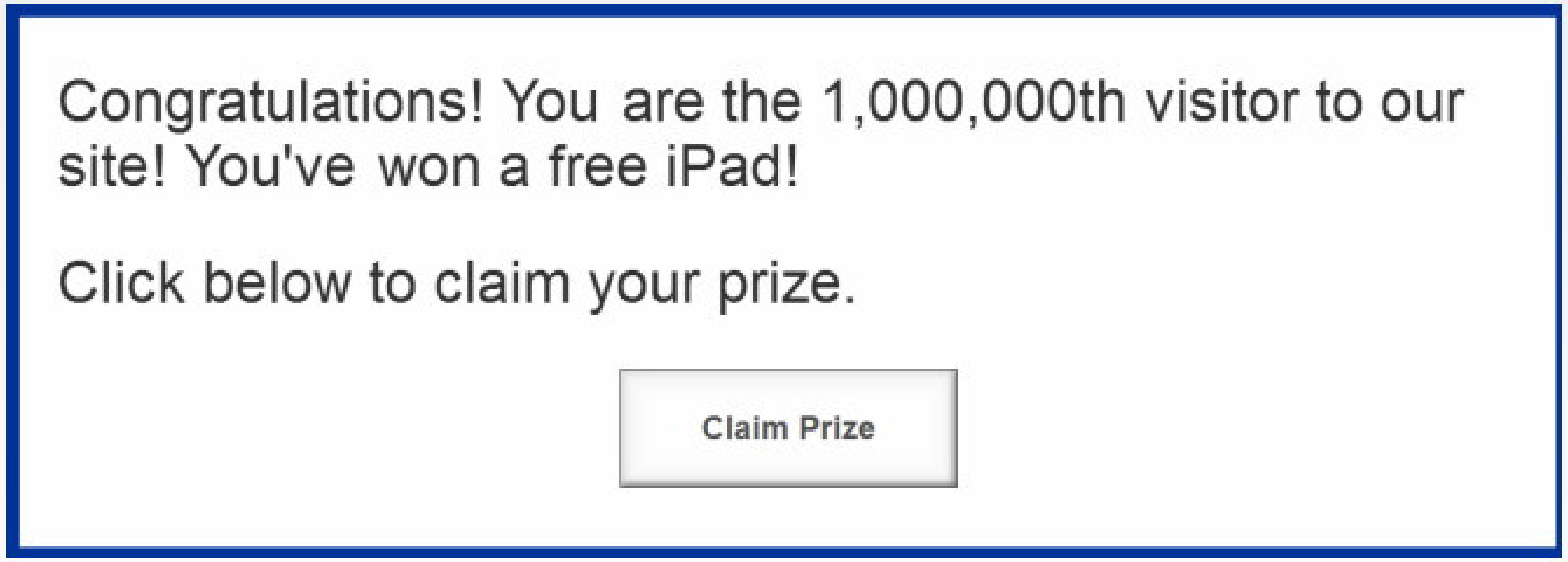
Safely Surfing the Internet

Don't Fall For It (2). The same thing applies for messages like those below:



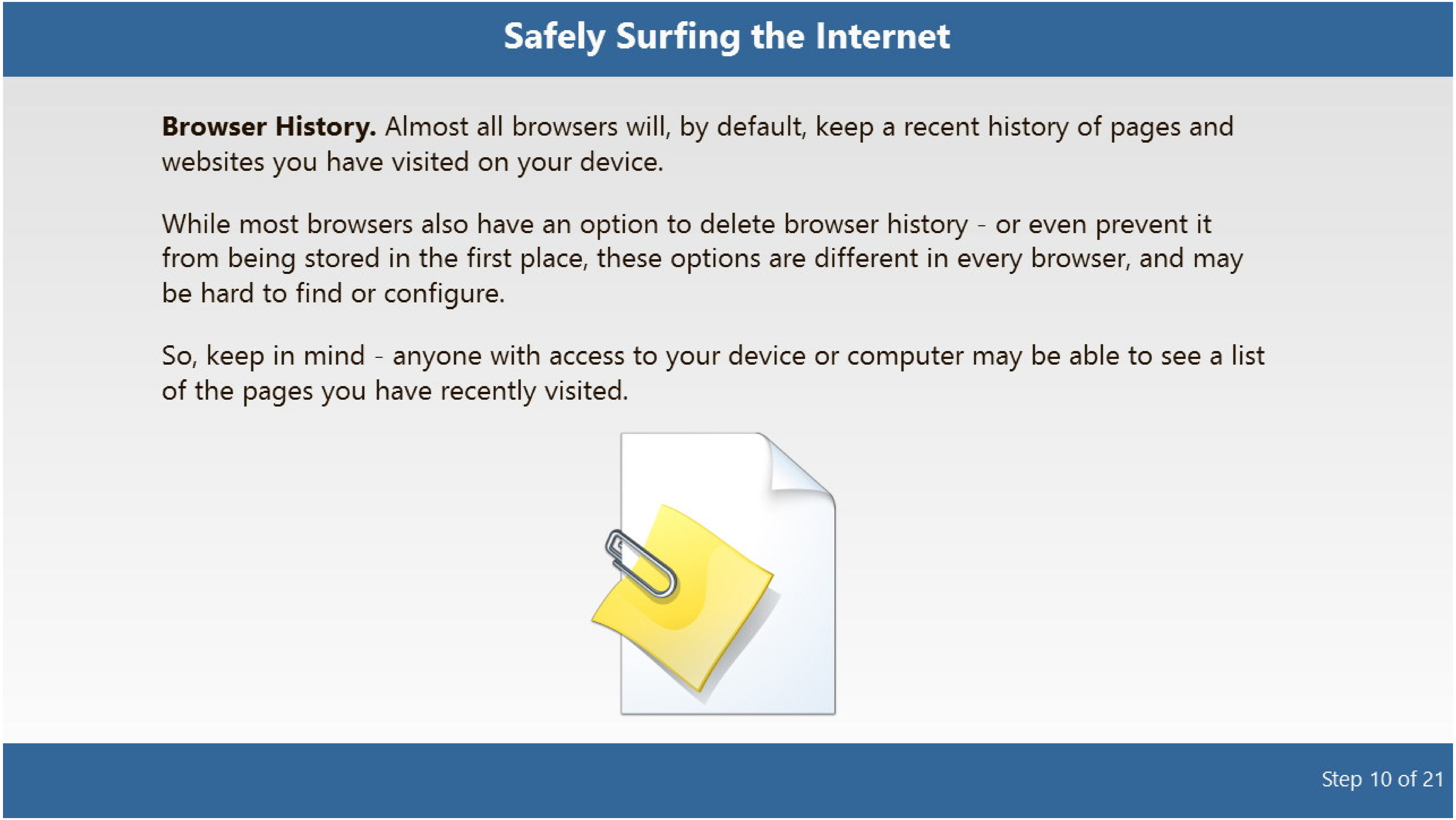
We've detected that your system is running very slowly.

Click Install below to speed your system up.



Congratulations! You are the 1,000,000th visitor to our site! You've won a free iPad!

Click below to claim your prize.



Safely Surfing the Internet

Browser History. Almost all browsers will, by default, keep a recent history of pages and websites you have visited on your device.

While most browsers also have an option to delete browser history - or even prevent it from being stored in the first place, these options are different in every browser, and may be hard to find or configure.

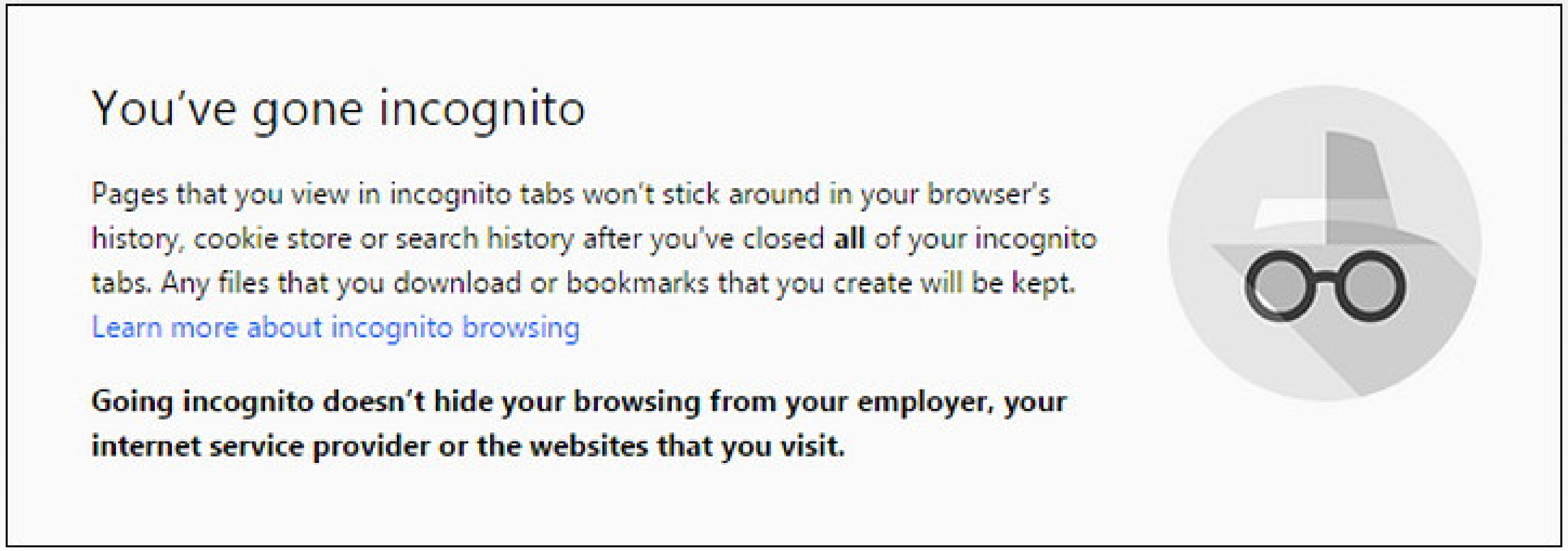
So, keep in mind - anyone with access to your device or computer may be able to see a list of the pages you have recently visited.

Safely Surfing the Internet

Incognito Mode. Most browsers these days have a mode called **Incognito Mode, Private Browsing,** or something similar. When this mode is invoked, any pages you visit will not be stored in your browser history. Generally, there is no record that you ever visited these sites.

Technically, however, this is not true. A computer expert, or your Internet Service Provider will still be able to determine what pages you have visited. But it will prevent most users from checking your browser history on your computer.

Below is a message you'll see if you run the Google Chrome browser in **Incognito** mode.



You've gone incognito

Pages that you view in incognito tabs won't stick around in your browser's history, cookie store or search history after you've closed **all** of your incognito tabs. Any files that you download or bookmarks that you create will be kept. Learn more about incognito browsing

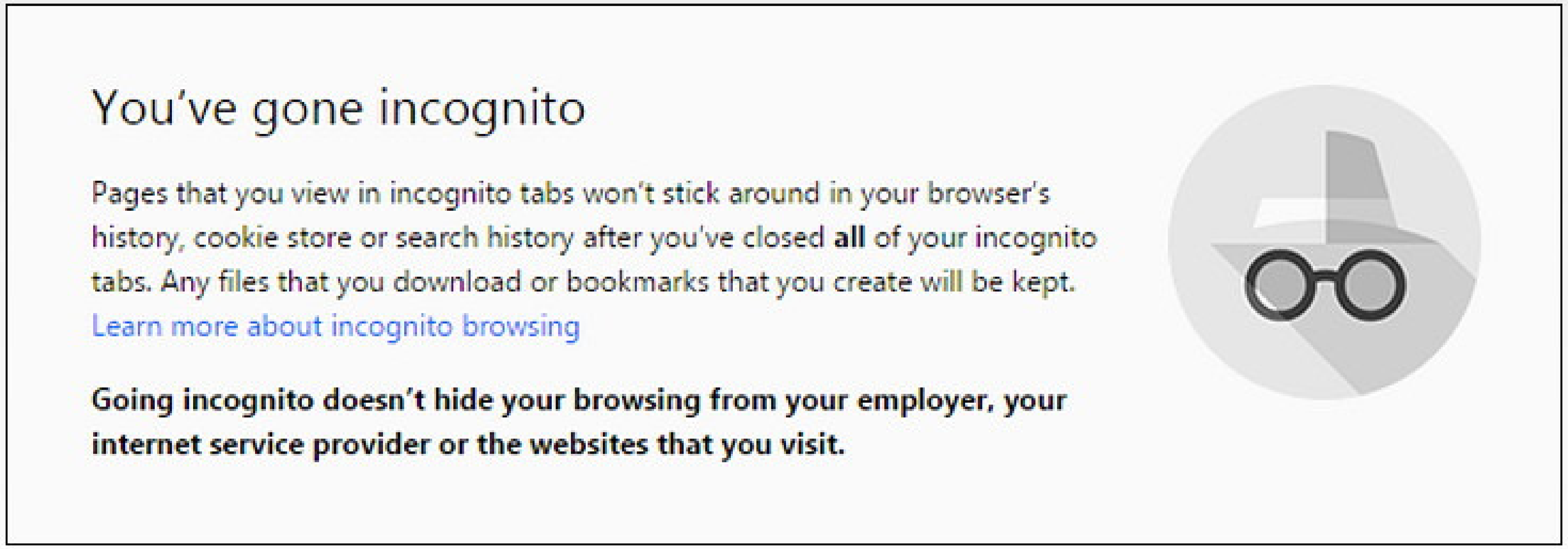
Going incognito doesn't hide your browsing from your employer, your internet service provider or the websites that you visit.

Safely Surfing the Internet

Using Incognito Mode. Read the instructions the browsers gives you if running in Incognito or private mode.

For example, to really keep your web history a secret from prying eyes, ensure you close all incognito or private browser windows before leaving your computer or or turning off your device.

In a moment, we discuss your **IP Address** - a kind of digital footprint left by every Internet connected device. Incognito or private mode will not hide this digital footprint.



You've gone incognito

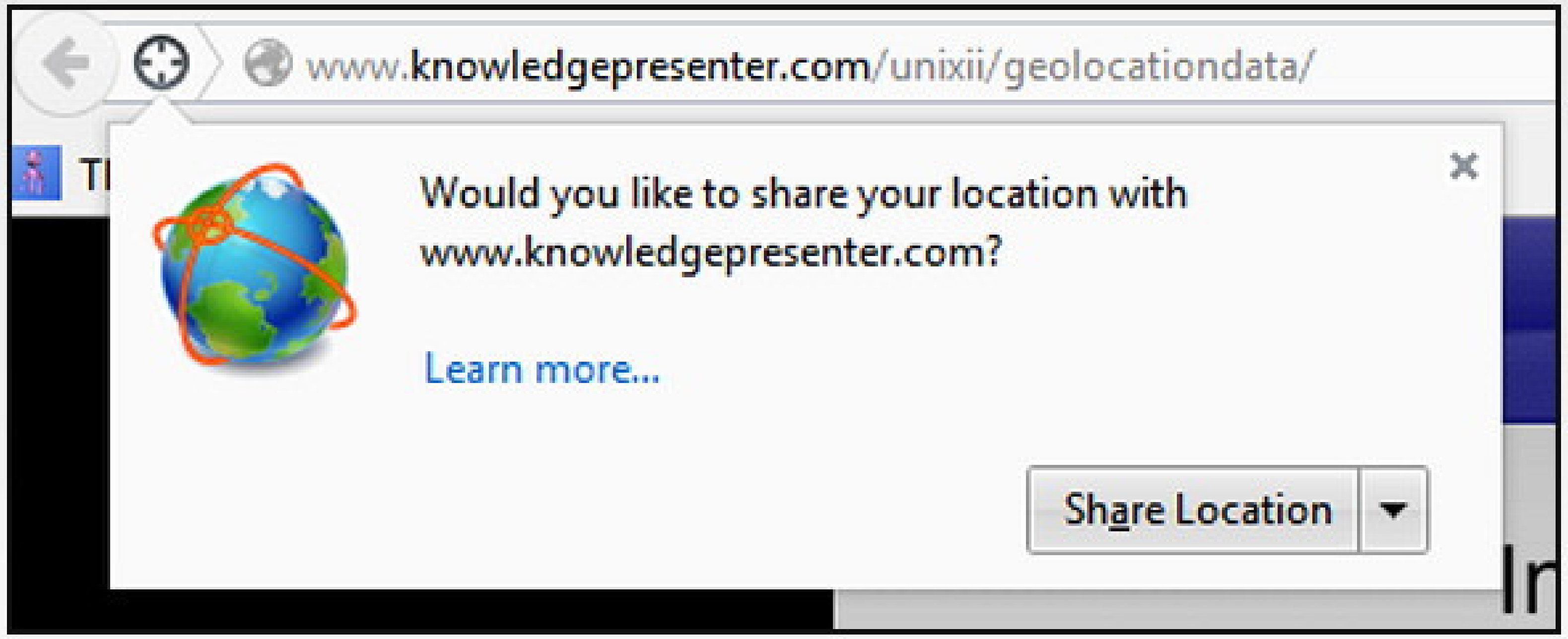
Pages that you view in incognito tabs won't stick around in your browser's history, cookie store or search history after you've closed **all** of your incognito tabs. Any files that you download or bookmarks that you create will be kept. Learn more about incognito browsing

Going incognito doesn't hide your browsing from your employer, your internet service provider or the websites that you visit.

Safely Surfing the Internet

Your Privacy. As computer technology develops, Internet browsers can do more and more. This can be a good thing, but also a bad thing.

Luckily, most browsers do the right thing - and ask for your permission to perform certain tasks. For example, if a website asks for your location, your browser may present you with a question, something like this:



www.knowledgepresenter.com/unixii/geolocationdata/

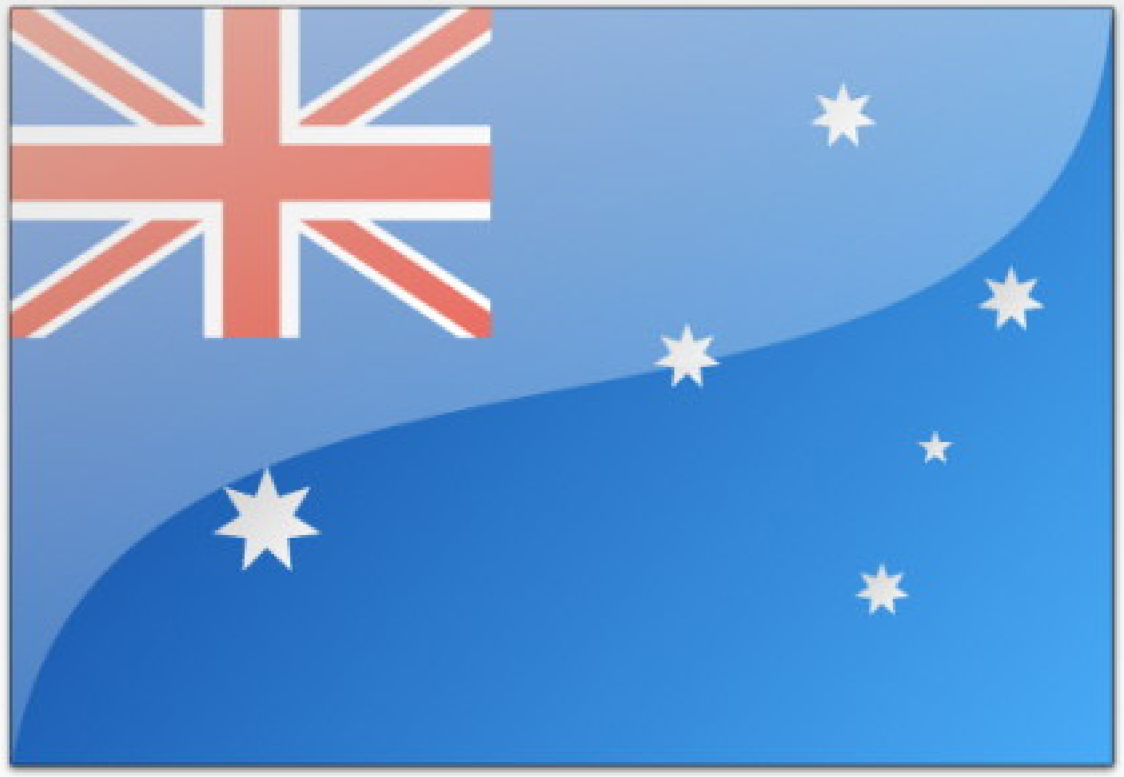
Would you like to share your location with www.knowledgepresenter.com?

It's up to you whether you want to allow a particular website to know your location. Sometimes it can be useful for you - the website may be able to provide directions to a location. Other times, or if you are not sure, you can simply refuse permission.

Safely Surfing the Internet

Your Location. To specifically - or very closely - find your location, a browser will ask permission on behalf of the website as to whether you want to allow this (as we saw on the previous step). However, this is not the only trick a website can use.

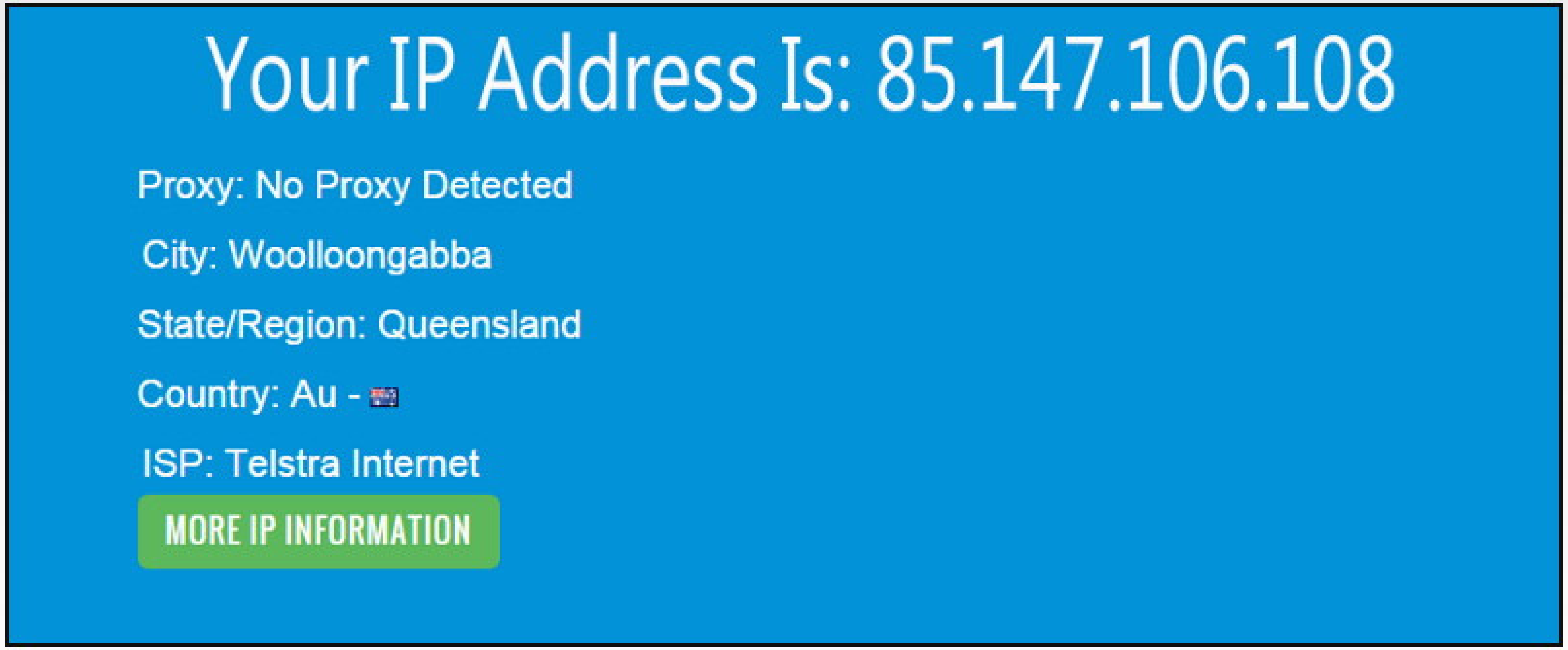
Every time you browse a website, that website can determine your **IP Address,** without your knowledge. Your **IP Address,** which looks something like *186.123.255.67,* is assigned by your Internet Service Provider. Every device or router connected to the Internet has such an IP Address.



Safely Surfing the Internet

Your IP Address. Using your IP Address, the website can use real-time geolocation software to find your location. At best, this is to the closest major city or town, not to your actual address. And it is not always accurate.

Using a website like **www.whatismyip.com,** you can try this yourself - below, you see an example of what this, or any, website can find out about you.



Your IP Address Is: 85.147.106.108

Proxy: No Proxy Detected

City: Woolloongabba

State/Region: Queensland

Country: Au - 🇦🇺

ISP: Telstra Internet

Safely Surfing the Internet

Your IP Address and Law Enforcement. A website can find your general location, and is far from exact, as we have mentioned.

However, if law enforcement needs to find you, they can (if the circumstances allow) take the the IP Address to your Internet Service Provider, and find out exactly where you are, and who you are.

Running your browser in Incognito or Private Mode will **not** prevent your IP Address from being captured.

Safely Surfing the Internet

What else can Websites Find Out About You? There are several things a website can find out you, without you permission. This includes:

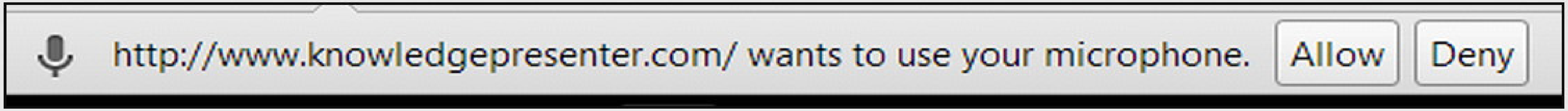
- The browser and browser version you are using
- The device or operating system you are using
- Your screen resolution
- Your language
- Your time zone
- Whether on a touch or mouse based device
- Variety of your device or computer capabilities

Safely Surfing the Internet

Why can Websites Find All This Out? Websites generally don't find these sorts of details out to invade your privacy. Generally, a website may need to know your screen resolution to format content correctly. It may provide extra facilities if you are using a tablet, or phone, rather than a computer, for example.

Safely Surfing the Internet

Asking for Permission. Other times, an Internet browser or app may ask for permission to use your webcam, or your microphone.



http://www.knowledgepresenter.com/ wants to use your microphone.

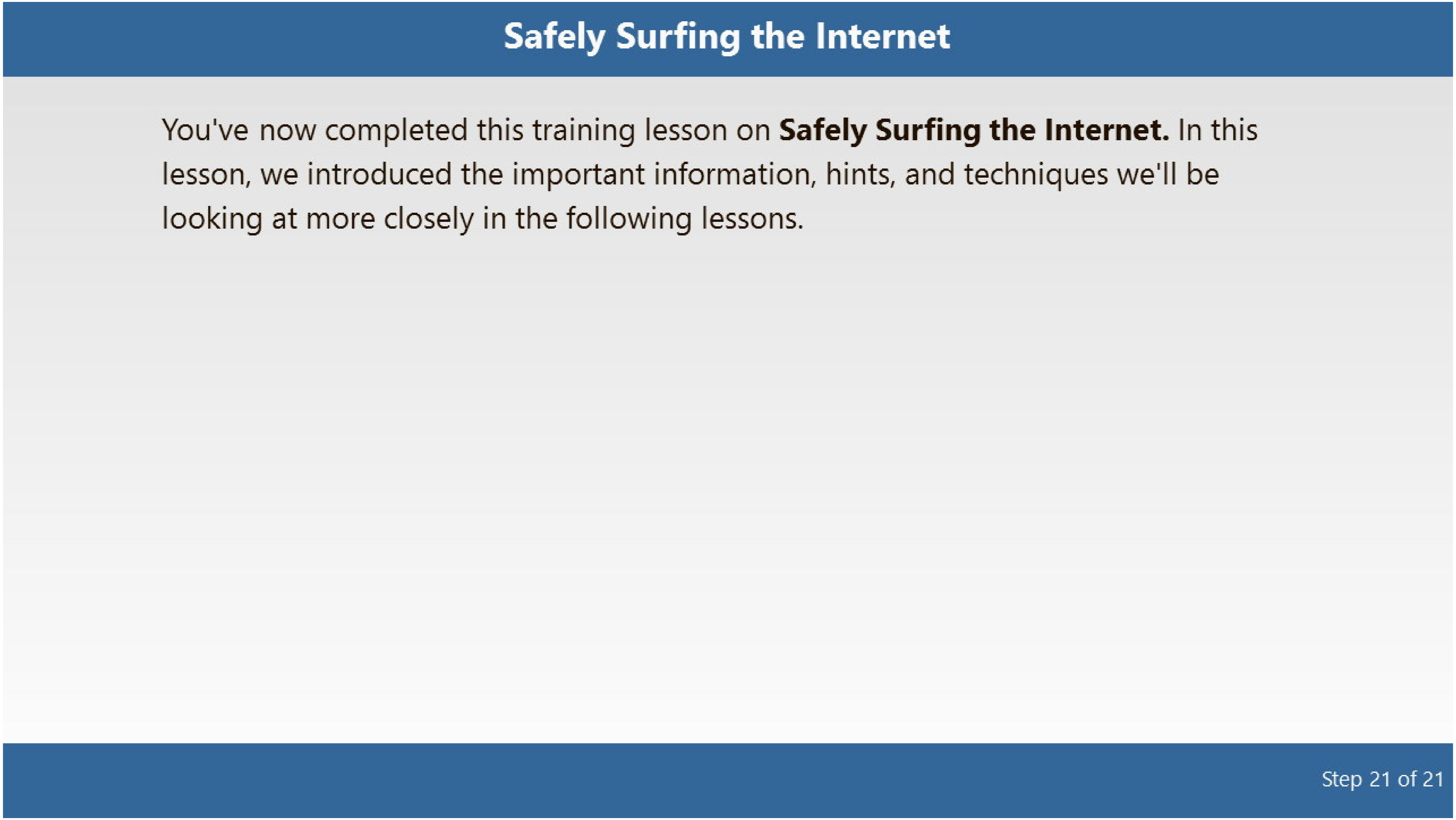
Again, unless there is a specific reason that the browser needs access to your webcam, microphone, or any other part of your computer that requires a question like this, you are best off refusing permission.

Safely Surfing the Internet

Popup Windows. Almost all browsers have the feature to block **popups.** Popups are unwanted and un-asked for new windows that can appear as soon as you browse to a new web page, usually displaying some form of advertising.

These are generally more annoying than dangerous - and that is why a popup blocker is generally activated by your browser by default. It may warn you that a popup window was blocked as it blocks them.

A popup blocker does not generally block all new windows from opening. If the window is opened as a result of a click, or a touch from you, then it is generally allowed to be opened without any warnings.



Safely Surfing the Internet

You've now completed this training lesson on **Safely Surfing the Internet.** In this lesson, we introduced the important information, hints, and techniques we'll be looking at more closely in the following lessons.