CENSUS COUNTS 2020

NEW AMERICA

Cybersecurity Best Practices For Organizations with Census Kiosks

The 2020 Census will be the first high-tech census and will be the first time there will be a widely available option to respond online (households will also be able to participate in the 2020 Census by phone or using the paper form). Stakeholders can feel confident that the Census Bureau is implementing the most up-to-date safeguards to protect households' responses. But, for organizations setting up census kiosks, there are also steps you can take to increase your own cybersecurity before you respond. This guide is designed to help stakeholders, households, and individuals take steps to protect themselves and their communities when completing the census form—and whenever they go online.

The following four sections offer some background and recommendations for increasing your cybersecurity. Section 1 reviews general hardware security. Section 2 reviews Wi-Fi security while taking a high-level look at the differences between private and public networks. Sections 3 and 4 review browser security and general information about phishing, respectively.

Personal Cybersecurity Practices

Section 1: Hardware Security

Hardware refers to the physical elements of technology—your cell phone, laptop, monitor, mouse, keyboard, and the electronic chips inside the devices you use. Software refers to the computer programs that run on your devices and that you interact with when you use technology (you wouldn't just want to stare at a blank screen all day!). Firmware is a specialized bit of software that helps your device carry out a specific purpose.

Hardware works along with firmware and software to run your devices, and it's important to make sure that the firmware and hardware are running well and up to date so that the software can function well and securely.

Use two-factor authentication on devices. Authentication is the act of securing hardware and systems from unintended users. Common authentication practices use passwords, fingerprint scans, face recognition, and external USB keys. Two-factor authentication means requiring two different kinds of authentication for a use to be granted access into the system. For example, you might set up your email system to require both a password and a verification code sent to your cell phone. Two-factor authentication makes it harder for malicious actors to access your devices.

Use hardware that is currently supported by the manufacturer. Older devices become less secure when they are no longer "supported" by manufacturers—which means that users are no longer provided with system updates and patches that respond to newer security threats. Devices that are less than four to five years old are usually still supported, but you can check with your manufacturer to be sure. For example, this **link**[1] provides a chart by Statista that shows how long Apple has supported different models of iPhones.

Install and activate antivirus, malware, and ransomware protections. Most devices come with these protections installed but often users don't activate them. These services protect devices from all-too-common attacks. Check with the manufacturer (for example, **Acer**, **Asus**, **Apple**, **Dell**, **HP**, **Lenovo**, and **Microsoft**) to see what protections they recommend for your system.

Install any outstanding manufacturer security updates. Make sure to keep security protections up to date. When you are notified about updates, don't put off installing them! When patches and updates are released, it often means a security "hole" has been identified. This means the period after a new patch is released is a common time to be targeted by malicious actors, because the security hole is common knowledge and bad actors know many users have not yet installed the update.

Replacing/fixing broken devices. Be sure the place you get your phone or computer fixed is a trusted or authorized retailer for your system. Check with the manufacturer (for example, **Acer**, **Asus**, **Apple**, **Dell**, **HP**, **Lenovo**, and **Microsoft**)to find a trusted or authorized retailer to repair your system. Faulty chips or hardware parts can also be used to breach your system.

Never leave hardware unlocked in public places. Don't leave your devices unlocked in public even for a few minutes.

Do not plug any unknown device into your device. Never plug in an unknown USB flash drive or external phone into to your personal computers to see what's on it. Avoid using promotional USB flash drives that are distributed at events or by untrusted entities. This is an easy way for malicious code to get on your machine.

Section 2: Wi-Fi Security

Private Wi-Fi Networks

Private Wi-Fi networks, such as home or work networks that are password-protected, are more secure than public, no-password-required networks.

Authentication protocols: When a device identifies a Wi-Fi network, look at the network's properties to find out what type of security it uses, specifically a version of Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, or Wi-Fi Protected Setup (WPS). The most secure and recommended protocol is called WPA2, which addressed a security concern with the older WPA system. WPS is the newest security method but has a major security hole and, even though it is newer, WPA2 is still the recommended protocol.

Wi-Fi Passwords: When setting up a Wi-Fi network, make sure you change the password from the default password, because those defaults are available online.

A strong Wi-Fi password:

- ➜ Has a combination of uppercase letters, lowercase letters, numbers, and symbols.
- ➜ Is as long as you can possibly remember. It is recommended to be at least more than 8 characters and ideally more than 12. A long phrase or sentence you can remember, with numbers standing in for some letters, may be a good way to go.

In addition:

- ➜ Change your password regularly. Set a schedule for how often you want to change your organization's passwords. Changing your organization's Wi-Fi password in March 2020 is the recommended minimum for the census.
- ➜ Do not reuse passwords. Wi-Fi passwords should not be used for anything else.

Service Set Identifiers: The service set identifier (SSID) is the name you see when connecting to a Wi-Fi network. When setting up a Wi-Fi network, change the default name to make it less likely that someone will connect to it by mistake, or that a malicious actor is able to guess it. Change it to something unique so that nearby users (or yourself) do not get confused on where to connect. For example, if your organization is near others and your network is "workwifi," some neighbors may use similar names and think your Wi-Fi network is theirs—or vice versa. Your device will try to connect to "workwifi" and if the first one it sees is not password protected it may connect to that essentially public wifi.

Your SSID should also be unique so that hackers won't be able to spoof or pretend to be your organization's network. If you leave a device's Wi-Fi on while out and about, it will look for networks to connect to. If a bad actor spoofs what a generic or out-of-the-box network looks like, they make be able to connect to your device.

Other General Tips for Private Networks:

- ➜ Enable your firewall.
- ➜ Keep your router's firmware up to date.
- ➜ Turn off remote administration if you enabled it.
- ➜ Mac addresses can be spoofed and easily obtained if the device has ever connected to a public network. Therefore, it is not enough to tell your network to only allow certain Mac addresses.

Public Wi-Fi Networks

Public Wi-Fi networks do not require a password. These are often found in places like coffee shops, airports, or public spaces. In general, these networks are not secure and not recommended.

If possible, switch to your data plan and avoid public Wi-Fi altogether. Your cell phone may also have a setting that allows you to use it as a secure Wi-Fi hot spot, which can be a good alternative in public settings.

If you are going to use a public network for completing the census questionnaire—or in general—here are some security tips:

- ➜ Make sure the open Wi-Fi you are using is being provided by the establishment. Attackers can set up a public Wi-Fi with an SSID (see above) that seems legitimate to trick people into connecting to them.
- ➜ Use a Virtual Private Network (VPN) if on public Wi-Fi. A VPN creates an encrypted connection on a public network. If you think of public Wi-Fi as a highway, using a VPN creates a tunnel for your data that is protected from the rest of the network. There are many VPN apps available for you to use.
- ➜ Use larger, well-known Wi-Fi networks, such as a large chain, rather than a small establishment's individual network.
- ➜ Read the terms and conditions when connecting to Wi-Fi. Make sure you know what data and permissions you are allowing the provider to get in exchange for letting you use their networks. Most "free" things are not truly free.
- ➜ Don't set your devices to automatically connect to available Wi-Fi. When you enable automatic connection your devices broadcast the connections it is looking for, which makes it easier for bad actors to spoof networks to gain access to you.
- ➜ Use all hardware and browser security tips found in this resource.

If your organization is setting up a network to assist your community in responding to the census, use the hardware and browser security tips found in this resource.

Section 3: Browser Security

When going online to use the Census Bureau's Internet Self Response portal to complete the census questionnaire, please use **supported browsers**[2] such as Internet Explorer, Safari, Chrome or Firefox. Check to make sure the version you are using is up to date. If you are not sure or if you need to update your browser, you can use the following links:

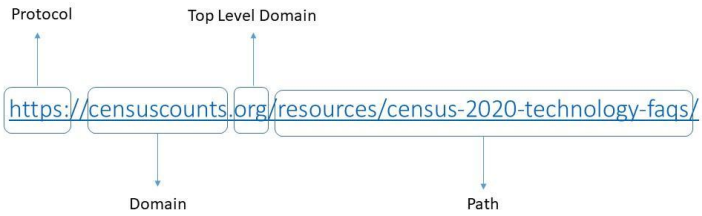
Internet Explorer
https://www.microsoft.com/en-us/download/internet-explorer.aspx

Safari
https://support.apple.com/en-us/HT204416

Chrome
https://support.google.com/chrome/answer/95414?co=GENIE.Platform%3DDesktop&hl=en

Firefox
https://support.mozilla.org/en-US/kb/update-firefox-latest-release

URL: Know the right URL, or website. Check 2020census.gov for the correct URL to complete your form online. Make sure you are checking the Top Level Domain (TLD) too! Just because the domain is the same (i.e., “censuscounts”), if the Top Level Domain is different, it is a different website! Look for .gov on the URL, it is the only TLD that the Census Bureau will use.



http vs https: Hypertext transfer protocol is more than just the beginning of a URL. It specifies how the device transfers information. Https stands for hypertext transfer protocol secure and means that data coming and going from the site is encrypted. Even if the data is accessed by a third party they won’t have the key to decrypt it. It is generally good advice to only use websites that are https not http. If you know a site is usually https and you are seeing http, you may be part of a person-in-the-middle attack and should leave the site immediately.

Search Engines and Social Media: Whenever you search for census-related materials on any site (search engine or social media), be sure to notice whether the results you are getting are advertisements. Often the first few items you see are paid ads (see images 1 and 2), and the actual results and websites you are looking for may show up below those ads.

Digital Ads: Before clicking any link from a digital ad, hover your mouse pointer over it to see the URL it links to (shown in the lower left-hand corner of the window). Use the URL information above to determine if that is the correct site you wish to visit.

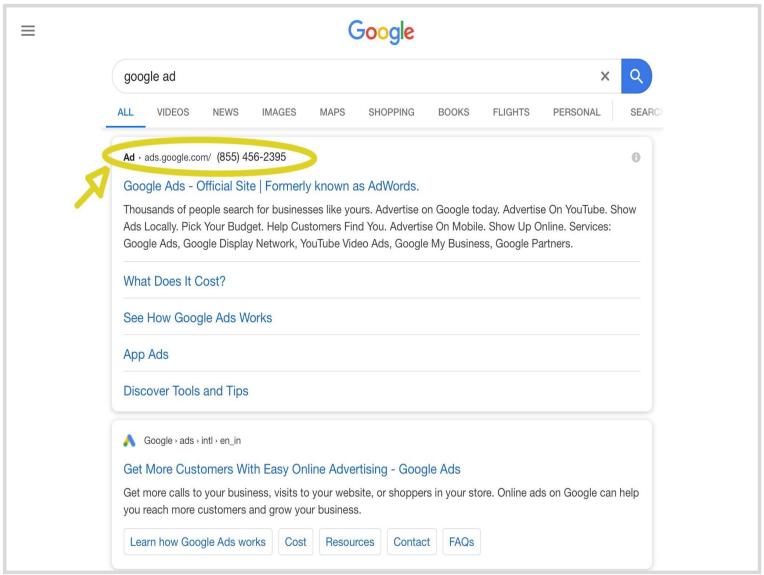


Image 1: Example of paid advertisement on Google

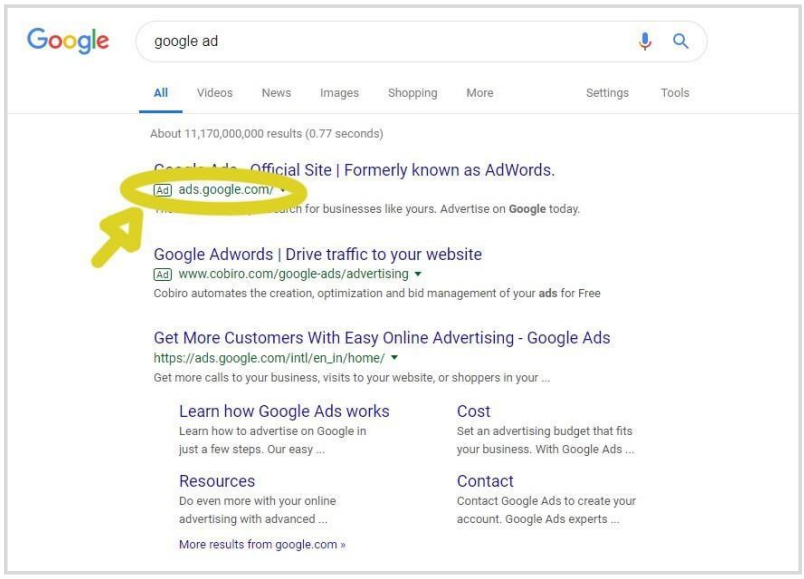


Image 1: Example of paid advertisement on Google

Section 4: Phishing Hints

"Phishing" is an act of tricking users to give away their information or create an entrance point for malware. This is done in many different ways:

1. False emails that ask you to click a link or download something
2. Fake phone calls asking for information
3. Attachments that give bad actors access to your data

Bad actors are essentially "fishing" for your data and it's important to protect yourself when you are online. That's one reason to be sure you're at the correct URL. But also be aware of the questions you are being asked. The Census Bureau will not ask for things like Social Security numbers, bank account, or credit card numbers—online or over the phone.

If you encounter a phishing scam, please report it! You can report it to the **Census Bureau**.[3]

References

PAGE 2

1. Richter, Felix. “How Long Does Apple Support Older iPhone Models?” Statista, 19 September 2019. Available at https://www.statista.com/chart/5824/ios-iphone-compatibility/.
2. “Fact Sheet: Questions and Answers for Stakeholders Supporting the 2020 Census.” U.S. Census Bureau, 16 October 2019. Available at https://www.census.gov/library/fact-sheets/2019/dec/guidelines-for-partners.html.
3. “Avoiding Fraud and Scams.” U.S. Census Bureau. Retrieved 10 November 2019. Available at https://2020census.gov/en/avoiding-fraud.html.

CENSUS COUNTS 2020

1620 L Street NW, Suite 1100
Washington, DC 20036

(202) 466-3434

censuscounts.org

@civilrightsorg

@civilandhumanrights