Fast Forward

Internet Safety

What is Internet Safety?

There's almost no limit to what you can do online. The Internet makes it possible to access information quickly, communicate around the world, and much more. Unfortunately, the Internet is also home to certain risks, such as malware, spam, and phishing. The importance of Internet safety in between a variety of information, personal data, and property protection is imperative. Internet safety is more important for users while accessing online banking services and shopping.

Being Safe Online:

Computers can often give us a false sense of security. After all, no one can physically harm you through a computer screen. But to stay safe online, you'll want to take a more cautious approach. Here's one way to think about it: Treat the Internet as you would a shopping mall. You probably wouldn't leave your car unlocked or give your credit card number to a stranger.

Fast Forward

Categories

1) Personal Security
    a. Online Scammers
    b. Automated Predators
2) Information Security
    a. Safe Sites/Scam Sites
    b. Avoiding Spam and Phishing
    c. Internet Browsing Security Features

Personal Security

The FBI's Internet Crime Complaint Center (IC3) received 351,937 complaints of online fraud in 2018, with $2.7 billion in reported losses—that's an average of over 900 per day at $7,672 per person.

According to the IC3, almost 40% of all internet crime victims are over the age of 50. –The most common reason? Willing to help others.

Tip: Make sure you know the person you are offering to help. Try offering to help with your time or goods before providing money.

Online Scammers come in a variety of forms. From fake websites, bogus pop-ups for security warnings, fake credit reporting sites, and scammers through emails. Never click on an ad that claims your computer is not secure, or make claims that are too good to be true.

Tip: By law, you're entitled to a free copy of your credit report once every twelve months. **AnnualCreditReport.com** is the only government-authorized website for ordering your free annual credit report, but the internet is full of imposter sites.

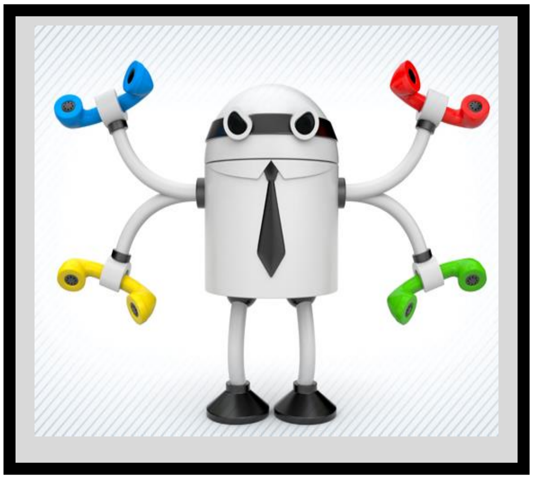
Automated Predators

Never provide your phone number online unless it is a safe site or on a website that you know.

If you answer the phone and hear a recorded message instead of a live person, it's a robocall. If you're getting a lot of robocalls trying to sell you something, odds are the calls are illegal. Many are also probably scams.

Scammers can fake the name and number that shows up, making it look like a call is from a government agency like the Social Security Administration or a local number. That's called spoofing.

Watch out for the IRS and Social Security calls. Some things to look out for during the call:



1) Unwillingness to provide name or location information.
2) Threats that seem excessive (calling the FBI to have you arrested).
3) Claims that you did something wrong and money will correct the problem.
4) The Social Security Administration will never call and ask for your social over the phone or ask you to pay any money.

What should I do if I get an illegal robocall?

Hang up. Don't press any numbers. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls, instead.

Information Security

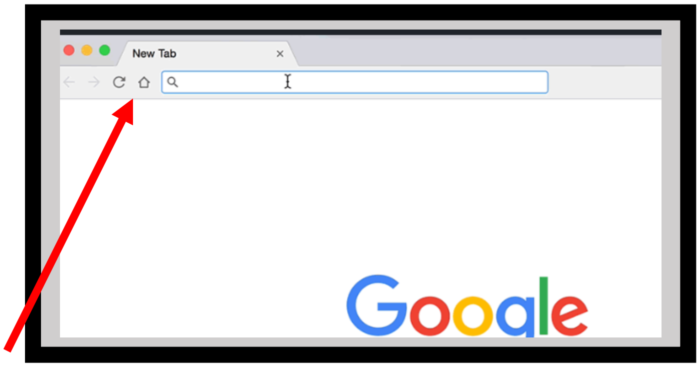
Being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this online in a safe manner.

How to Keep Information Safe

Knowing the Difference Between Safe and Scam Sites

Ways to Determine if a Website is Fake, Fraudulent, or a Scam

1.) Pay Close Attention to the Web Address



Most people do not pay attention to the address bar at the top of the page. Especially once they click on a link. This is a huge mistake. The address bar contains a ton of vital information about where you are and how secure you are there. Get into the habit of occasionally glancing up there whenever you visit a new page.

2) Check Connection Security Indicators

When you search online, websites automatically show either "HTTP" or "HTTPS" before the www. on a website.

Any search, email, shopping, etc. done via HTTP is sent in plaintext and can be intercepted, manipulated, stolen—you name it.

Look for "HTTPS" or a lock icon before any website before you enter personal or banking information. –More Below!

3) Check the Spelling of a website

It sounds simple, but it is easy to forget. Scam sites often come from other seemingly safe sites. After clicking on a link, look at the address bar. Does the website have "HTTPS"? Is it spelled correctly?

Remember, websites end in ".com," ".org," ".edu," or ".gov"

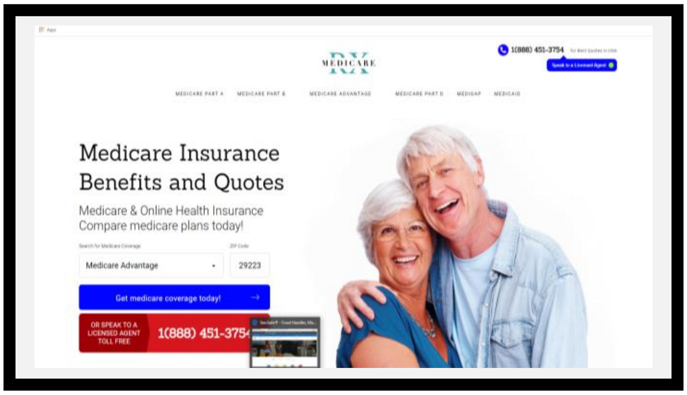
Take a look at these popular fake websites:

www.bankofamerican.com –Extra letter on the website

www.amason.com –Spelling error in the website

www.ssa.com -Ending of website.

Social Security, DSS, City websites, etc. end in ".gov." Only government departments can have a website with this ending.



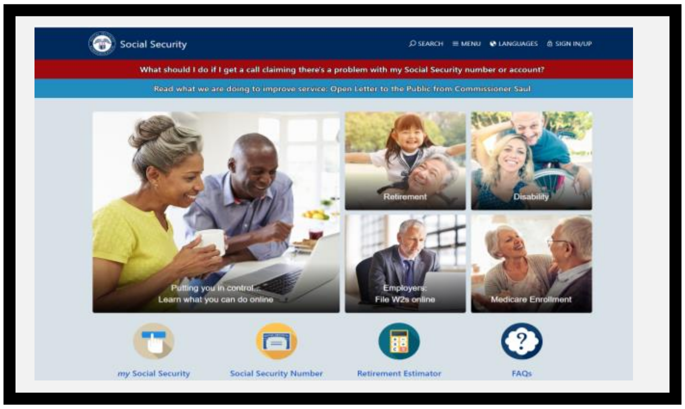
Medicare Insurance Benefits and Quotes

Medicare & Online Health Insurance
Compare medicare plans today!

Medicare Advantage

29223

www.ssa.com



What should I do if I get a call claiming there's a problem with my Social Security number or account?

Read what we are doing to improve service: Open Letter to the Public from Commissioner Saul

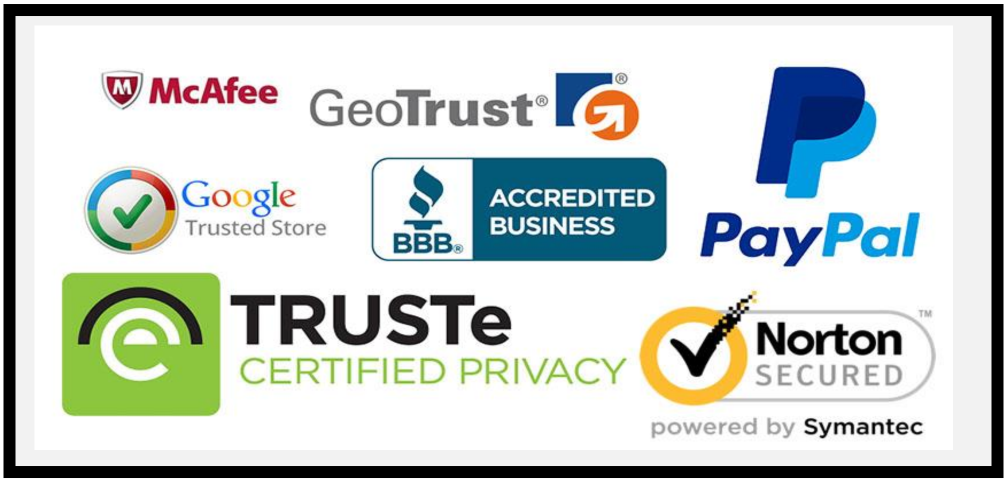
Putting you in control...
Learn what you can do online

www.ssa.gov

4) Look for Trust Seals

When a company or organization makes a substantial investment in its customers' security, they typically want a little bit of credit for it. That's one of several reasons that trust seals exist. You've probably seen more than a few trust seals in your time on the internet.

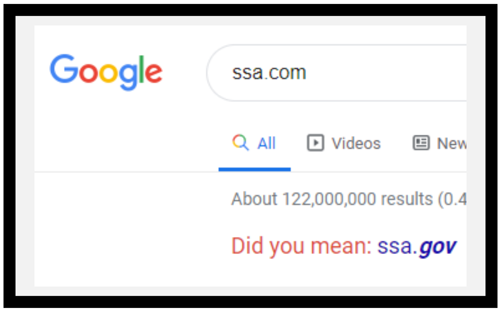
They look like this:



Trust seals are commonly placed on homepages, login pages, and checkout pages. They're immediately recognizable, and they remind visitors that they are secure on this page.

5) Google It!

If a company or a website seems too good to be true, or it seems a little off, type it into Google (www.google.com) and see if it comes up as a safe site or a scam. If the website appears to be wrong, Google will suggest the correct site.



ssa.com

About 122,000,000 results (0.4

Did you mean: ssa.gov

Avoiding Spam and Phishing

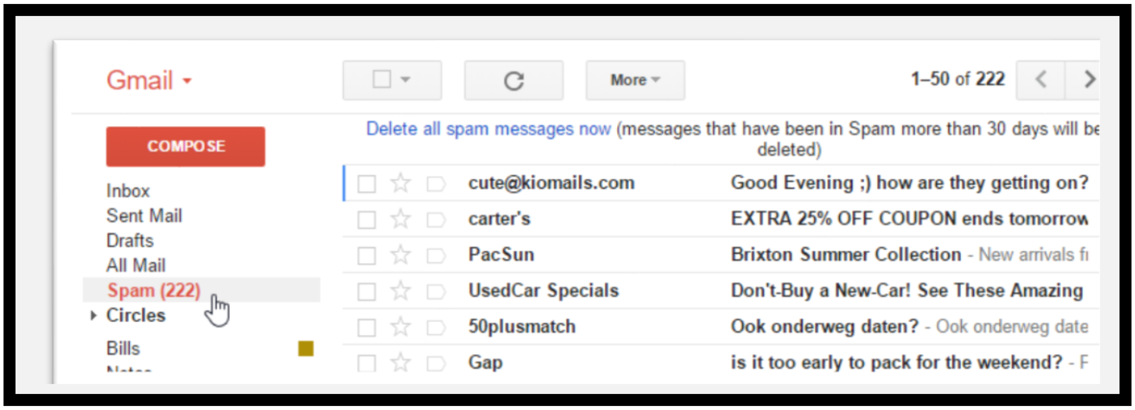
Protect yourself from email scams, malicious software, and identity theft, you'll need to understand how to identify and prevent potentially dangerous content in your inbox,
including spam and phishing attempts.

Dealing with Spam

Spam, also known as junk, messages can clutter your inbox and make it more challenging to find the emails you want to read. Even worse, spam often includes phishing scams and malware, which can pose a severe risk to your computer. Fortunately, most email services now include several features to help you protect your inbox from spam.

Spam filters

Whenever you receive an email, most email providers will check to see if it's a real message or spam. Any likely spam messages will be placed in the spam folder, so you don't accidentally open them when checking your email.



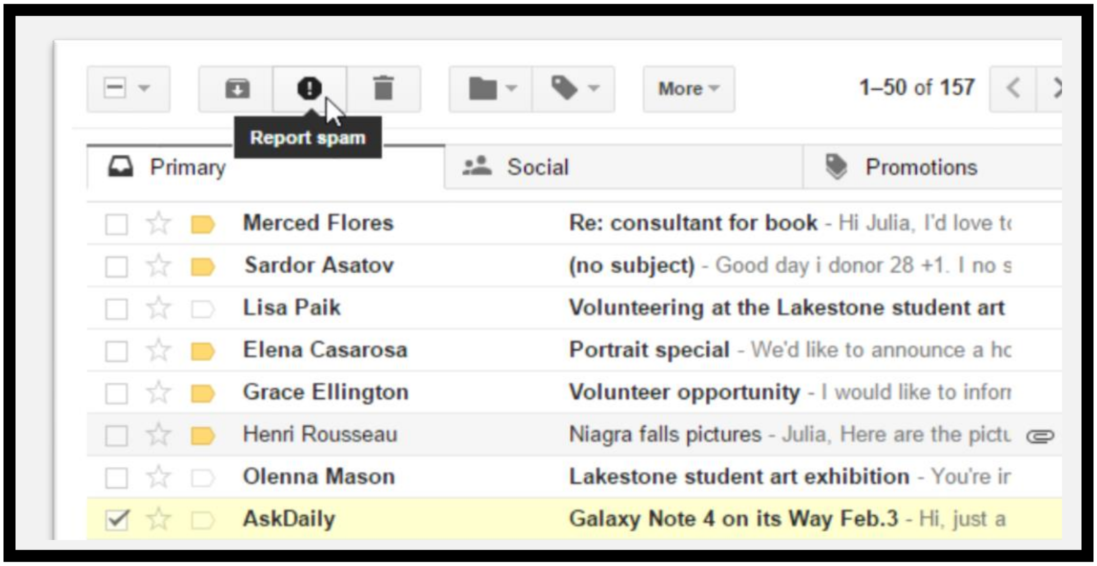
Delete all spam messages now (messages that have been in Spam more than 30 days will be deleted)

cute@kiomails.com	Good Evening ;) how are they getting on?
carter's	EXTRA 25% OFF COUPON ends tomorrow
PacSun	Brixton Summer Collection - New arrivals fi
UsedCar Specials	Don't-Buy a New-Car! See These Amazing
50plusmatch	Ook onderweg daten? - Ook onderweg date
Gap	is it too early to pack for the weekend? - F

Spam-blocking systems aren't perfect, though, and there may be times when legitimate emails end up in your spam folder. We recommend checking your spam folder regularly to make sure you aren't missing any relevant emails.

Fast Forward

Many email services also have a feature you can use to mark emails as spam. In Gmail, you can select the message and click the Mark as Spam button. This helps your email provider filter out these types of messages in the future.



□ ☆	Merced Flores	**Re: consultant for book** - Hi Julia, I'd love t
□ ☆	Sardor Asatov	**(no subject)** - Good day i donor 28 +1. I no s
□ ☆	Lisa Paik	**Volunteering at the Lakestone student art**
□ ☆	Elena Casarosa	**Portrait special** - We'd like to announce a hc
□ ☆	Grace Ellington	**Volunteer opportunity** - I would like to infor
□ ☆	Henri Rousseau	Niagra falls pictures - Julia, Here are the pictu
□ ☆	Olenna Mason	**Lakestone student art exhibition** - You're ir
☑ ☆	AskDaily	**Galaxy Note 4 on its Way Feb.3** - Hi, just a

Phishing

Phishing scams are messages that try to trick you into providing sensitive information**.** These often appear to come from a bank or another trusted source, and they'll usually want you to re-enter a password, verify a birth date, or confirm a credit card number. Phishing messages may look real enough at first glance, but it's surprisingly easy for scammers to create convincing details.

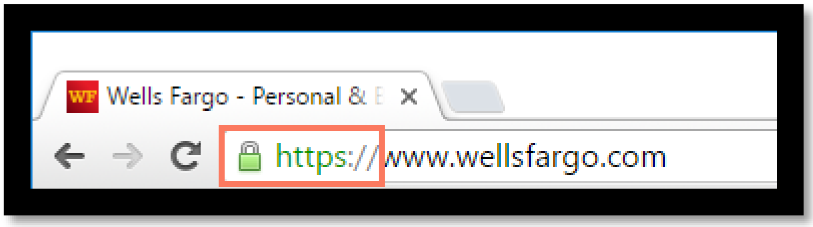
Fast Forward

Internet Browsing Security Features

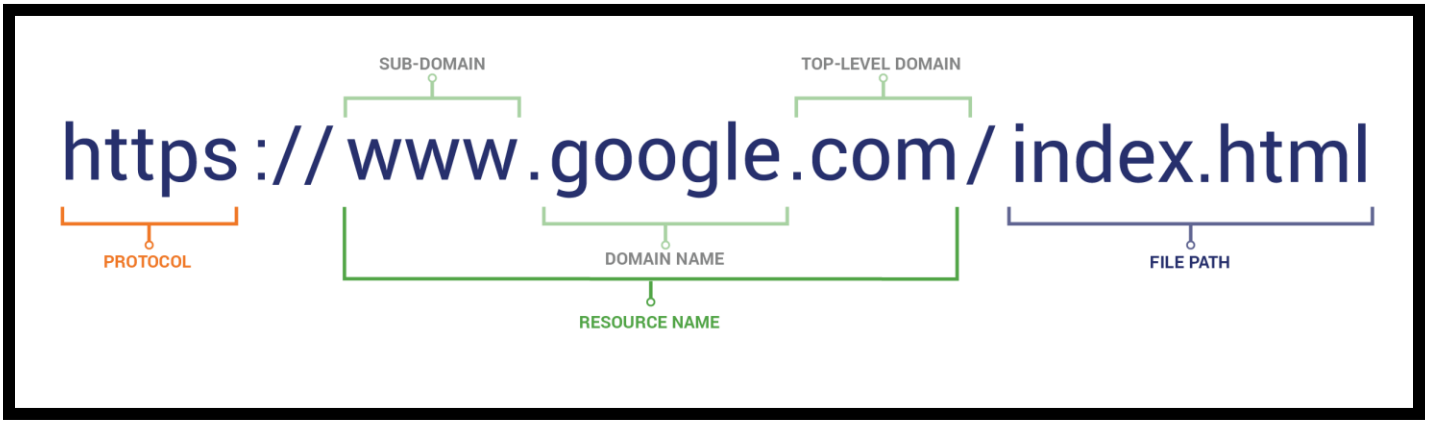
Your computer faces different threats whenever you browse the Web, including viruses, malware, and spyware. The good news is your web browser has a lot of built-in security features to help protect your computer.

Look at the security symbol

Some websites will display a lock symbol in the address bar. This is most commonly seen with certain types of websites, like online stores and banking sites. This means the website is using an **HTTPS** connection, which makes it safe to enter your personal information.



You won't see this symbol on all sites, and that's OK—not all websites need this extra layer of security. However, you should avoid entering any sensitive information, such as your credit card number, if you don't see this symbol in the address bar.



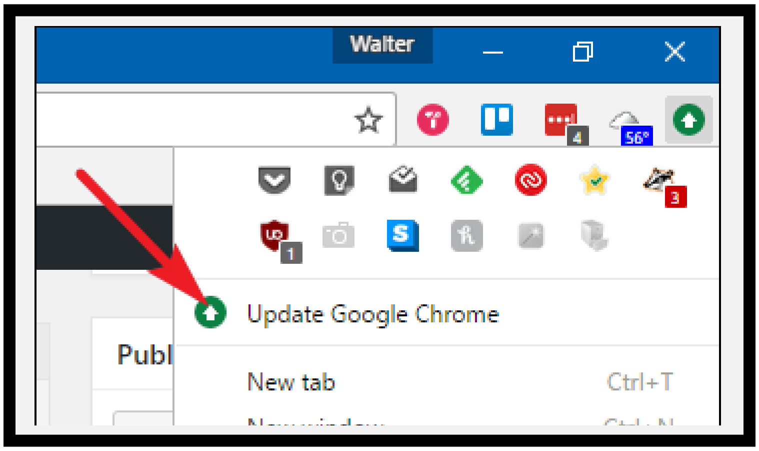
Fast Forward

Update your browser regularly

New viruses and malware are created all the time, so it's essential to update your browser regularly. Your browser will usually notify you when it has an update available, but you always have the option to update manually. In this example, we're updating Google Chrome to the most recent version, but the exact update procedure will vary depending on your browser.

Updating Chrome Browser

If Chrome has an update, there will be an "up arrow" icon in the right corner of your screen. Click on the arrow, and then click "Update Google Chrome."



Internet Explorer and Edge update when your computer runs security updates. You do not have to click any extra buttons to update.