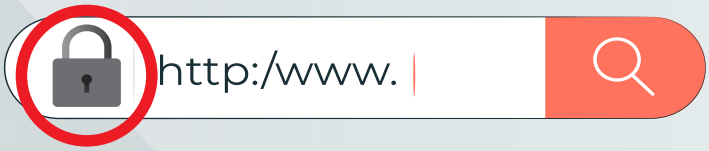
LFC
LOAVES, FISHES & COMPUTERS

Connecting Seniors with Technology
Internet Safety Guide

This Internet Safety Guide will help protect your computer from viruses, hacking, scams and more.

1. Internet Browsing/Browsing the Web

Make sure the website you visit is secured. Always look for the little lock on the search bar at the beginning of the website link, like in the image below, this ensures a safe website.



2. DO NOT Share YOUR Personal Information with anyone

1. Your Birthdate
2. Your Bank Account Number
3. Your Credit Card Numbers
4. Your ATM Pins
5. Your Social Security Number
6. Your Medicare or Medicaid Numbers
7. Your Passwords of any account, etc...

Keep all this information private, so that nobody gets access to it. There are many threats online. Unfortunately, hackers are just waiting for a chance to steal data from users.

3. Create Strong Passwords

All Passwords need to be hard to guess. To make a strong password you should use a mix of the following:

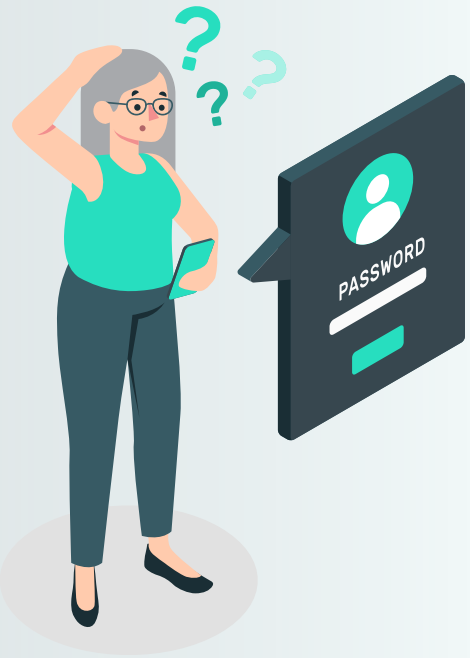
1. Make it at least 8 characters long
2. Use Upper and lower case letters
3. Have at least one symbol, (ex. #@!%)
4. Have at least one number.

GOOD Password Examples:

- Coffee$627
- Dancing?091
- C@stl3#69
- Pam45#$Link

Do not use as passwords:

1. Social Security Numbers
2. Any Birthdates
3. Pet's Names
4. Your children or your own name
5. Or any other private information.



4. Protecting Your Passwords

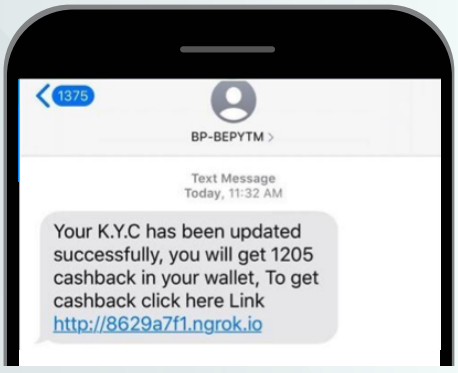
Write down the website address and your password so you remember them. Put this sheet of paper in a safe place. Be sure to tell a trusted family member or friend where that paper is!

NEVER share your passwords with anyone, including people who pretend to be from the Social Security Administration/SSA, Medicare, Doctor's Offices, Banks and anyplace that you may visit online or in person. People from Government Agencies will NEVER ask you for your Password.

5. Beware of scams on your computer, tablet & SmartPhone

Scams are everywhere, so you need to stay away from them and ignore any suspicious activity on the internet.

One of the most popular scams are via email. **NEVER open an email from someone you don't know or whose name you don't recognize.**



NEVER open emails that are forwarded to you even if these are from someone you know because you can inadvertently click on a link or get your email forwarded to a scammer's address.

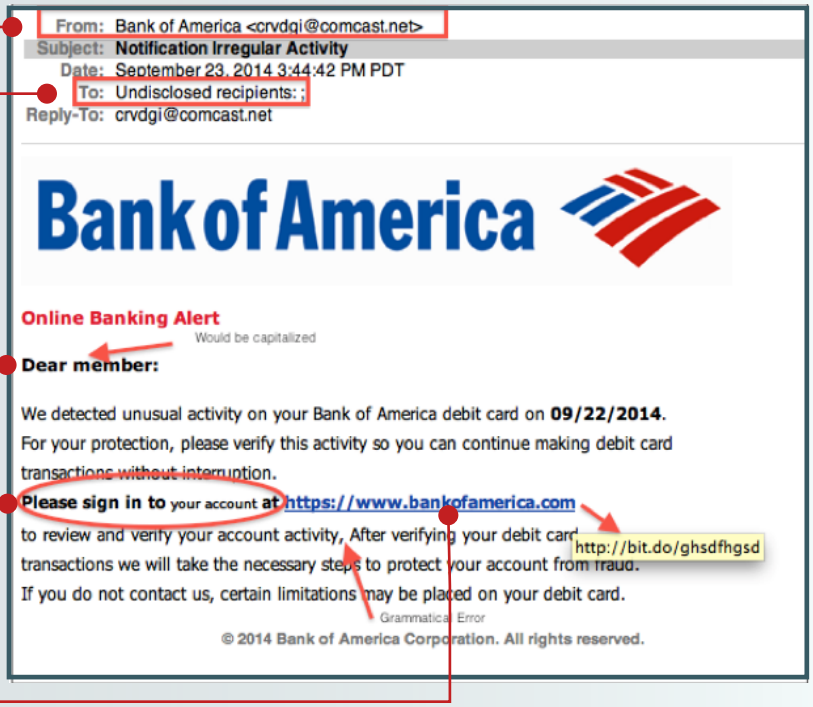
Emails like the ones in the following image are just trying to get users to click on their links so that they can either steal your personal information and data or install viruses on your computer or device.

Fake emails

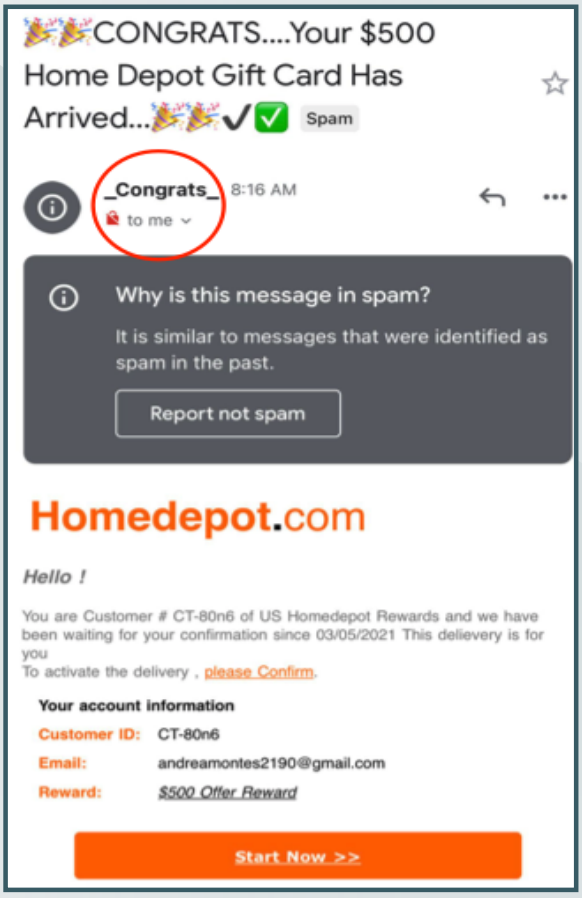
This image is a good example of how to spot a fake email.

Always look at:

- The **sender's** email address
- Check who were this email's **recipients.**
- Check for **grammatical errors**
- Be **suspicious** of the instructions.
- Hover over the **link** to ensure that it is the same as the one typed in the email



- You can contact the sender--your bank for example, to **verify if it sent this message.**



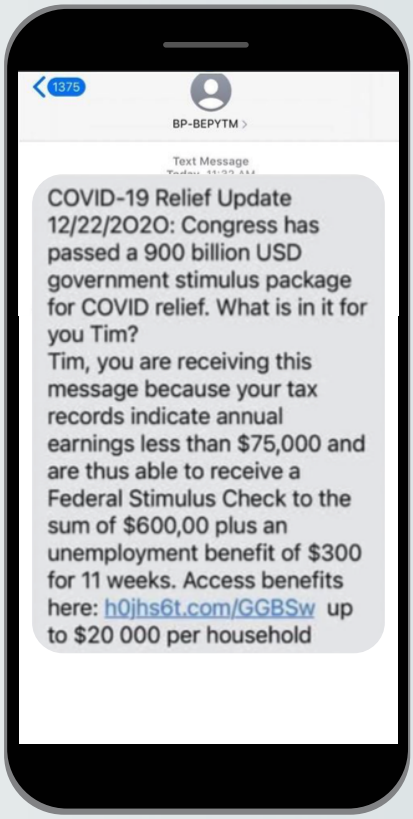
This is another example of fake emails.

Offers **too good to be true** are always a red flag.

If you receive emails claiming to be a **prize you won**, delete the email immediately.

These are scams trying to get you to give your information by clicking on the link.

You can also check where the email comes from, by clicking on the dropdown arrow marked in the red circle on the image.



Scams via text message.

Similar to fake emails, the new trend is to send scams via text message.

The image on the left is an example of how hackers are taking advantage of the current pandemic to steal information.

Messages also take advantage that people are waiting for their stimulus checks or unemployment benefits.

If you receive a text message like this, please delete them and **NEVER click on the link attached to the message.**

5. Always have an Anti-Virus software active on your computer.

If you are using a computer or Laptop that works on the Windows System, **you must have an antivirus** program in order to stay safe.

Chromebooks and Apple computers **DO NOT need antivirus software**.

chromebook

Antivirus software can be expensive, but **there are many that are free**. For example: Avast and McAfee

Many Internet Providers can also help with antivirus software, companies like **AT&T and Xfinity offer free antivirus** as long as you have service with them.

McAfee™

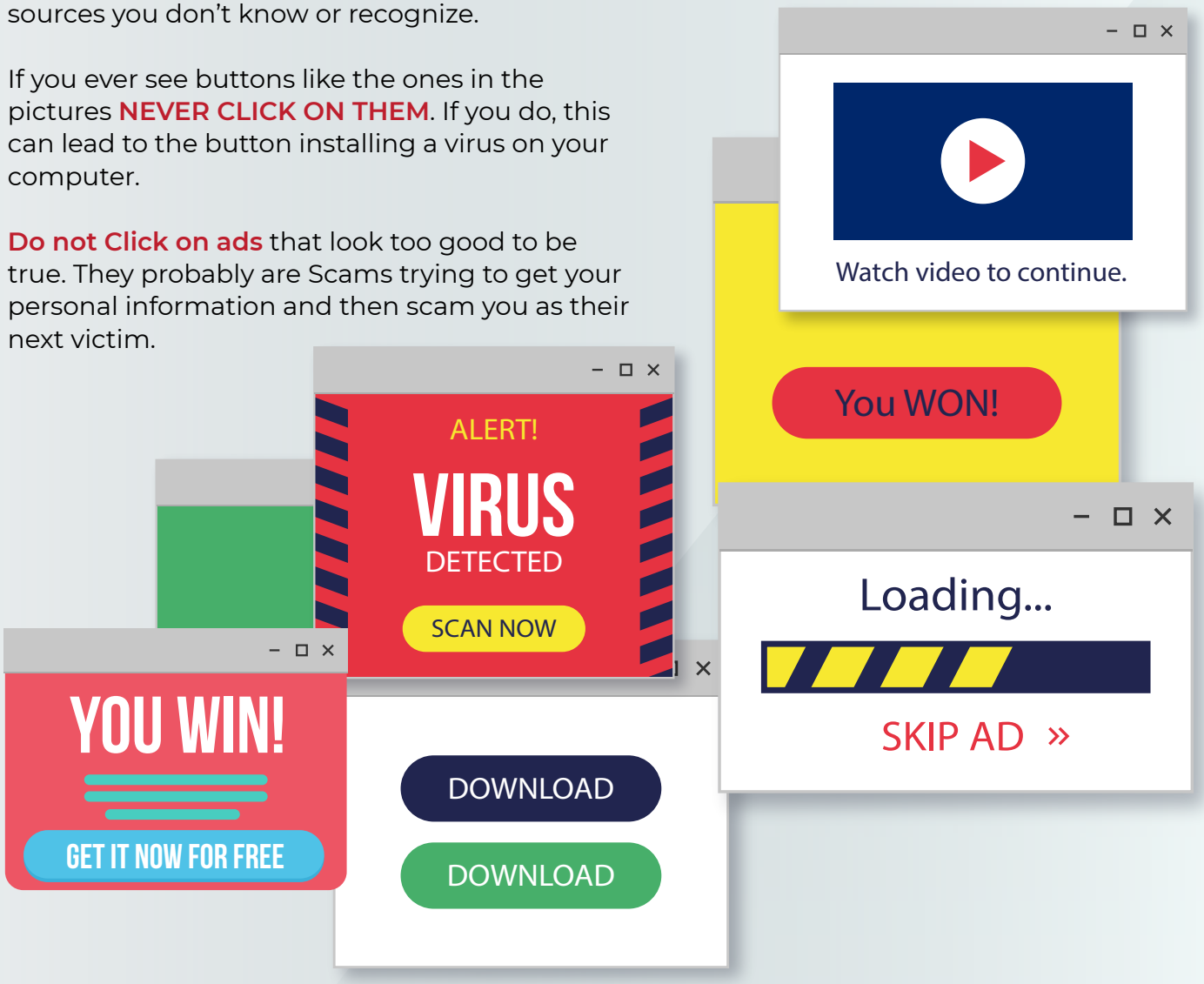
avast

6. Do Not Click or Download Content from Unknown Sites or Sources

Never click on a button or arrow to download anything from the internet that comes from sources you don't know or recognize.

If you ever see buttons like the ones in the pictures **NEVER CLICK ON THEM**. If you do, this can lead to the button installing a virus on your computer.

Do not Click on ads that look too good to be true. They probably are Scams trying to get your personal information and then scam you as their next victim.



7. Find More information Internet Security

There are many safe sources where you can learn more about Internet Safety. Here is a list of the most trusted sites for you to explore:

https://www.consumer.ftc.gov/
https://www.connectsafely.org/seniors/
https://www.aarp.org
https://staysafeonline.org
https://usa.kaspersky.com

QUICK TIPS INTERNET SAFETY

Don't Visit Unsafe Websites

Ignore Email Text Messages From Unknown Senders

Use Strong Passwords

Never Click Suspicious Links

Protect Your Private Information

Do Not Dowload Content From Unsafe Sites

Keep Your Antivirus Updated

LFC
LOAVES, FISHES & COMPUTERS

https://loavesfishescomputers.org

aaa
Monterey County
Area Agency on Aging