



(646)758-6606

support@candootech.com
candootech.com

Top Tips for Staying Safe Online

Staying safe online is important now more than ever. The FBI's Internet Crime Complaint Center (IC3), received more than 68,000 complaints in 2019 from victims over age 60 who experienced losses of more than \$835 million. In 2021, consumers reported losing more than \$5.8 billion to fraud. This was an increase of more than 70 percent over the previous year. At Candoo Tech, we want to protect you and your personal information. Here are 5 quick tips to stay safe online.

Tip 1: Be Cautious of Phone Scams

Phone scams occur year-round but tend to increase around the holidays. They often pretend to be a representative from a known agency or organization. Common disguises that scammers use include:

- The IRS
- The Social Security Administration
- The Police
- A relative
- An unknown charity
- A charity you have donated to
- A well-known company like Microsoft, Amazon, or Apple

If you receive a call from the above groups or anything that seems suspicious, please tell them you will call the organization back directly and hang up.



(646)758-6606

support@candootech.com
candootech.com

As a rule of thumb, it is best practice to not give personal information out on the phone including (but not limited) to your address, banking information, social security number, and passwords to a caller you do not know.

And, NEVER allow someone you don't know into your computer unless you have a pre-scheduled appointment that you have requested in advance.

[Read more about gift card scams here.](#)

Tip 2: Be Cautious of Email Scams

Email scams are common around the holidays and the main purpose is to gain access to personal information including credit card information, usernames, and passwords.

It is common for these emails to be disguised as emails from your bank, a credit card company, an app, an online payment website, or an online store. They can even include the company's logo!

Here are some tips to help you avoid email scams:

- Look up the company's customer service line and call to confirm if you received an email saying:
 - they've noticed suspicious activity
 - multiple failed login attempts
 - asking you to confirm personal information
 - claim there is an issue with your account
 - or ask you to make a payment
- Avoid opening or downloading any attachments in the email
- Make sure to read the link before clicking because often the link may be a character or two off from the real company's website. If you're unsure if a link is safe, it is best to not click it.



(646)758-6606

support@candootech.com
candootech.com

- Ignore and delete emails claiming that you won something free, gift cards, or vacations because they are likely malicious.

Tip 3: Use Strong Passwords

A great way to protect your personal information is to use strong passwords when creating accounts. Below is a list of some best practices for creating strong passwords.

- It is best to use lowercase and uppercase letters and a special character like ! or @ in your password
- The longer your password, the better!
- Avoid using personal information like your birthday or family member's name
- Make sure it's easy to remember
- Write it down in a safe place.
- You may want to explore a [password manager](#) to help you stay organized. This is a secure way to store passwords and also give a loved one access to your passwords safely.

Tip 4: Backup your Data

If you accidentally click or download a malicious link, we want to make sure that we can help you recover all your data (documents, pictures, videos, etc.) It is a best practice to regularly back up all your data on all your devices including smartphones, tablets, and computers. You can use an external hard drive or backup to a cloud storage.



(646)758-6606

support@candootech.com
candootech.com

Tip 5: What to do if you think you have been hacked

Remain vigilant for any suspicious activity on any of your credit cards or accounts- especially around the holidays

If you suspect suspicious activity on any of your credit cards or accounts, alert the organization's customer service line! They will be able to advise you on the next steps to help re-secure your account and information.

If you do fall victim to a scam and think someone has accessed your computer, disconnect the device from the Internet as soon as possible and call a professional to check for and get rid of Malware.

Actions you can take

- Report any suspected fraud at reportfraud.ftc.gov
- FBI Internet Crime Complaint Center [IC3.gov](https://ic3.gov)
- The Ultimate Internet Safety Guide for Seniors (2022) safetydetectives.com
- Add your number to the *Do Not Call List* by calling 1-888-382-1222 or by visiting donotcall.gov
 - This prohibits reputable companies from making sales calls to you.

Candoo is here to help you!

Call us at 646-758-6606 or email: support@candootech.com