

ONLINE SAFETY

LEARN WITH CLAIRE

HOW SAFE IS USING MY PHONE INTERNET

CONNECT THROUGH 4G/5G OR WI-FI

Safari is designed to protect your information and enable you to choose what you share. Use Safari settings to remove and block data that websites can use to track you in Safari.

To view these preferences, choose Settings > Safari.

Prevent Cross-Site Tracking

Some websites use third-party content providers. A third-party content provider can track you across websites to advertise products and services.

With this option turned on, tracking data is periodically deleted unless you visit the third-party content provider.

When Fraudulent Website Warning is enabled, Safari will display a warning if the website you are visiting is a suspected phishing website.

When Private Browsing is enabled, Safari doesn't remember the pages you visit, AutoFill information, and your open tabs aren't stored in iCloud. Websites can't modify information stored on your device, so services normally available at such sites may work differently until you turn off Private Browsing.



CAN MY IPHONE BE HACKED

HOW TO MAKE & MANAGE PASSWORDS

PRO TIP: YOUR APPLE ID CAN SAVE THEM FOR YOU

What's a strong password: Strong passwords are longer than eight characters, are hard to guess and contain a variety of characters, numbers and special symbols. The best ones can be difficult to remember, especially if you're using a distinct login for every site (which is recommended). This is where password managers come in.

Your Apple ID can store passwords for you:

go to **Settings > Passwords > AutoFill Passwords**, and check that **Autofill Passwords** is turned on.

For credit card information,* go to **Settings > Safari > Autofill**, and check that **Credit Cards** is turned on.

Open Safari.

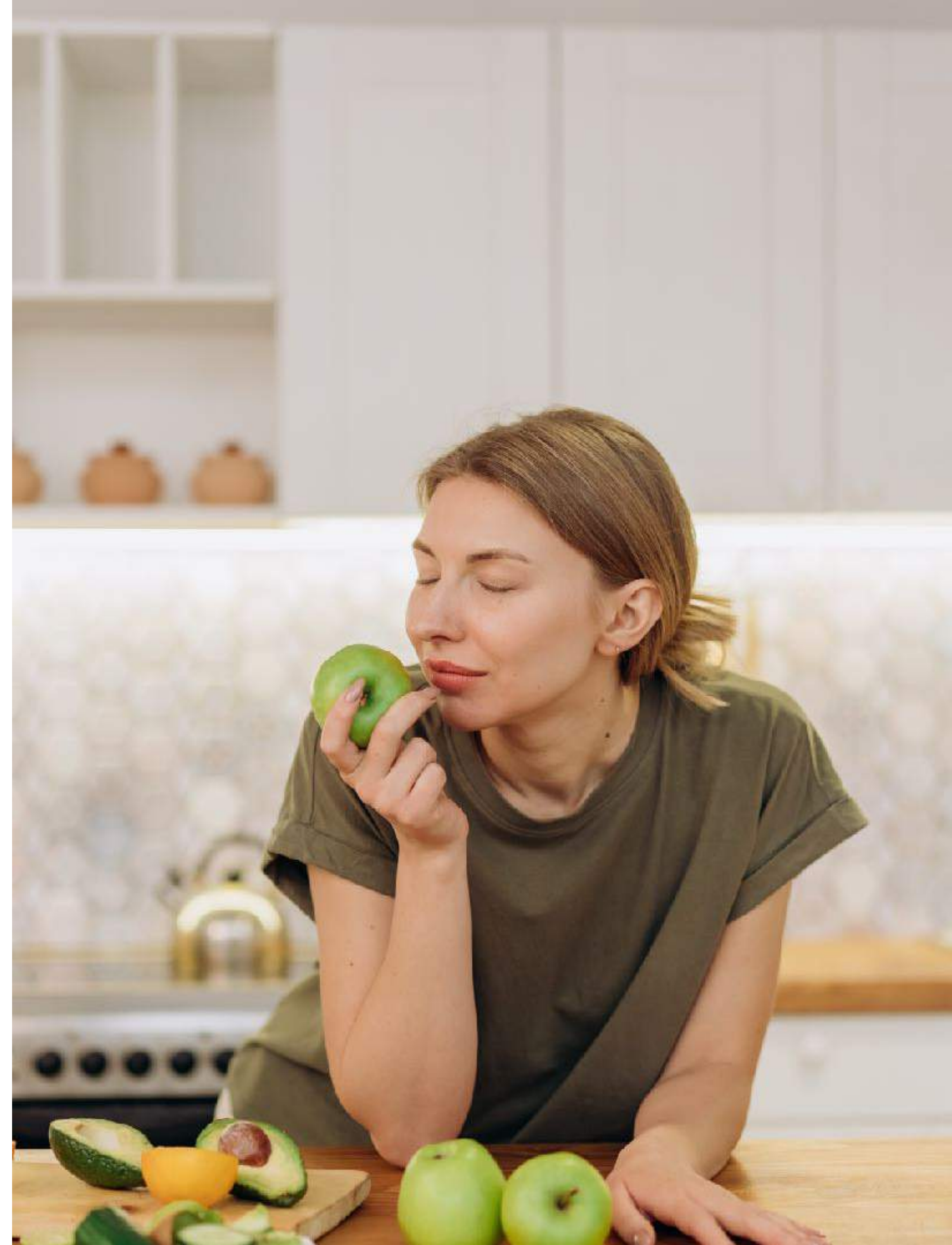
Alternatively, A trusted password manager such as 1Password or LastPass can create and store strong, lengthy passwords for you. They work across your desktop and phone.

ANTI VIRUS SOFTWARE

SKIP IT

First, iOS products don't offer any (that's not saying someone won't try to sell it). There really isn't any malware (viruses) that can be produced on a traditional iPhone / Mac users device

If you have a Windows computer at home and have a family member that may open suspicious emails or links, using Windows Defender or Norton is advised.



GOOD RULES TO FOLLOW

THESE WORK WELL FOR ALL THINGS INTERNET

Before you open an E-mail / Facebook message / Text Message

- **Do you recognize the sender**
- **Is your email provider / phone / computer warning you about the contents or the sender**
- **Do you recognize the email address / number / account it's from**

When in doubt, delete and contact the person/company directly



**BUT CLAIRE...I CLICKED
THE LINK!**

THAT'S GENERALLY PRETTY OKAY, DID YOU ALSO THEN DOWNLOAD ANYTHING OR ENTER YOUR PASSWORD? IF SO, DELETE THE PROGRAM AND CHANGE YOUR PASSWORD AS SOON AS POSSIBLE.

SHOULD I TRUST GEEK SQUAD?

MAYBE

Geek squad is a reliable and expensive option when you need help with your computer.

They are safe and generally pretty honest.

If you are a Mac user, you can visit the Apple website and they can help/fix your computer remotely!



FACEBOOK SAFETY & FRIEND REQUESTS

WHAT CAN YOU DO

First, make sure you followed our previous slide and created a strong password.

Next, make sure you are posting to your friends list and not publicly

What's my biggest threat on Facebook? Never. Ever. Give out your personal information to anyone over the internet this includes but is not limited to: your bank account, your credit card numbers, or your social security number. When in doubt? Say, I appreciate the information and I will call the company directly to pay my balance.

Why do I get random friend request from strangers? There is a large combination of fake accounts used to bolster statistics and scam artists. Decline them all.


Hannah Bouckley
Edit Profile

- News Feed
- Messages 4
- Events 3
- Saved 4

 Update Status |  Add Photos/Video

What's on your mind?



 Friends ▾

Post

This post is now hidden from your
Why don't you want to see this pl




Many reasons to like Wolf Ha
'fit' to be such a heavy breath
have nailed the look of portra

a bit too
at. They

Who should see this?

 **Public**
Anyone on or off Facebook

 **Friends**
Your friends on Facebook

 Friends except Acquaintances

 Only Me

 Custom

OTHER FACEBOOK TIPS

BEING SAFE IS SMART

Don't share future vacation plans

Check sources before you share / read articles

Post copy and paste status updates

You've seen these status updates that have been floating around Facebook for years:


Facebook is going to start charging on February 21st and unless you want to get charged you need to post this status update saying you do not agree to being charged for the service. You also need to go pet a unicorn while wearing a Speedo and rollerblades.

You get my drift....

8 SMART CYBERSECURITY HABITS


Learn more at:

<https://security.ucop.edu/resources/security-awareness/habits.html>

1  Think twice before clicking on links or opening attachments.


2  Verify requests for private information.

3  Protect your passwords.

4  Protect your stuff.
Lock it up or take it with you.

5  Keep your devices, browsers and apps up to date.

6  Back up critical files.

7  Delete sensitive information when it's no longer needed.

8  If it's suspicious, report it!

USE SOCIAL MEDIA AS A HELPFUL RESEARCH TOOL.

LOOK UP LOCAL BUSINESS, THEIR RATINGS, AND THEIR SERVICES.

USE LOCAL COMMUNITY GROUPS FOR ASSISTANCE AND ADVICE

A woman with long dark hair, wearing a brown fur jacket and a white pleated skirt, is walking away from the camera on a snowy path. She is carrying a young boy in a red hoodie on her back. She is also holding the hand of a smaller child in a colorful floral snowsuit. The path is covered in snow and leads through a wooded area with bare trees. There are wooden railings on either side of the path.

**GOODBYE FOR NOW
AS ALWAYS, FEEL FREE TO EMAIL ME AT
CLAIRE@AMPLIFY7.COM FOR ANY HELP**