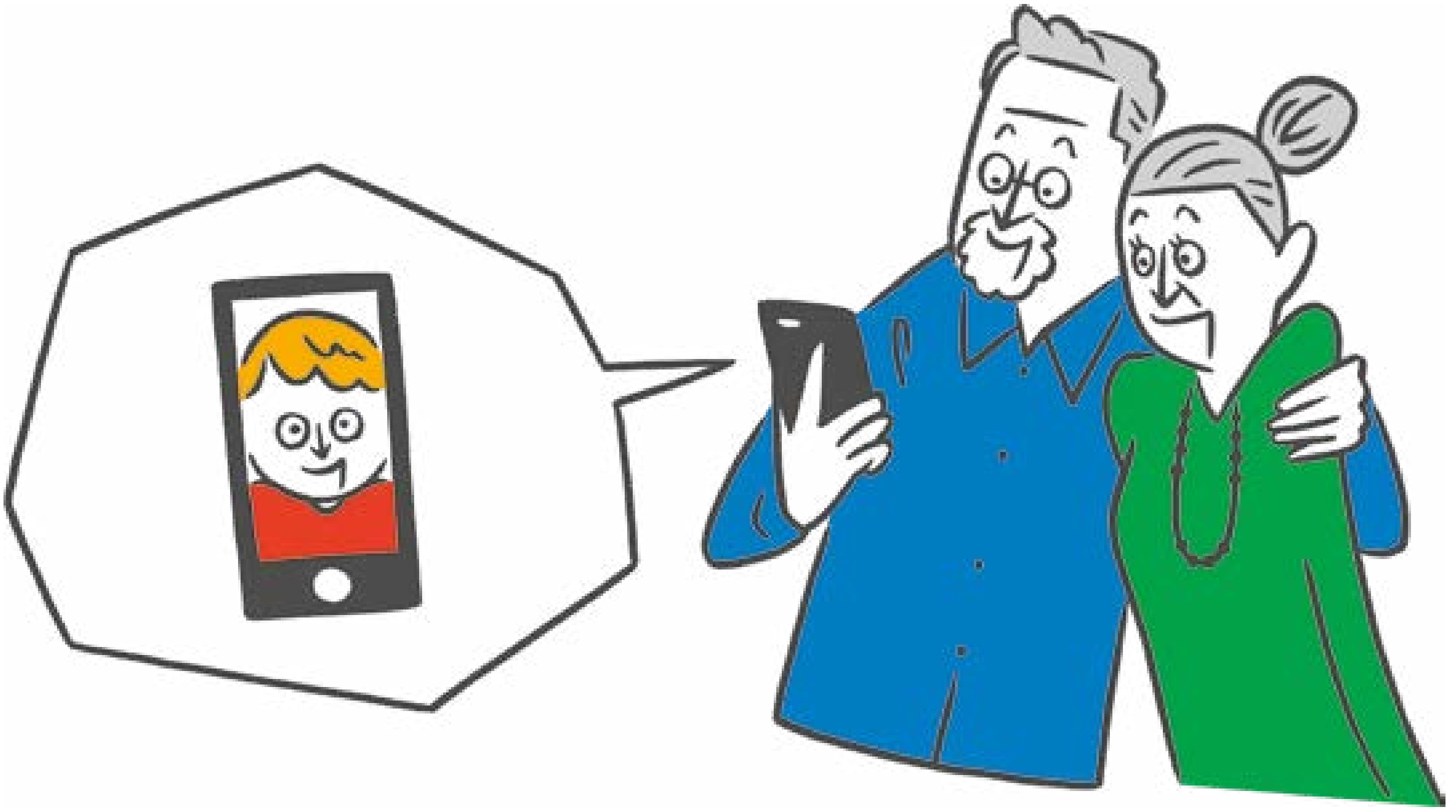
Online Safety Guide for Seniors

Some useful tips to help you navigate the Internet more safely.



Google

Introduction

The Internet makes it easy to get information on any subject, complete everyday tasks, and stay connected to the ones you love. You can communicate instantly with friends and family through email, messaging, and video chat, as well as share photos and videos with them.

With so many online businesses and services, the world is literally at your doorstep. The Internet allows you to compare prices across different supermarket chains, purchase groceries online, and have them delivered to your house.

The Internet is also a great research and learning tool, allowing you to expand your knowledge on your favourite subjects. You can learn a new language, build new skills or discover exciting opportunities in your local community.

The Internet is a fascinating place to learn, communicate, and get things done, but just like in the offline world, it's important to learn how to stay safe as you do these things. This guide will help you become more aware of common online scams and provide useful tips to help you navigate the Internet more safely.

Index

Terms Worth Knowing

There are some terms that you should know while you read through this guide and spend time online. If you wish to learn more about a particular term, be sure to research it online or ask your friends and family.

Topic General Knowledge

Term	Definition
Browser	You use it to access the web. The most popular ones are Chrome, Firefox, Safari, Internet Explorer and Edge.
Email	Electronic mail.
WiFi	The technology that allows you to connect to the Internet wirelessly.
SMS	Text messaging service available on most mobile phones.
Attachment	A file sent along with an email message.
Download	To obtain a file (such as an app or a program) through the Internet for storage in your phone or computer.
Upload	To transfer a file to a server or to the cloud – the opposite of download.
Log in	To enter your username and password to identify yourself and gain access to your online account.
Log out	The opposite of logging in. An important thing to do after using a public computer or someone else's device to access your account.
URL	Web address. Examples include google.com or gmail.com.

Topic Online Safety

Term	Definition
Malware	A term that encompasses computer viruses, Trojan horses, worms, adware and other malicious programs.
Social engineering	When someone tries to trick you into doing something dangerous online, such as downloading malicious software or sharing personal information.
Phishing	Remember the rich prince who wanted to transfer millions of dollars to your account? Well, that was a phishing email.
Impersonation	When an online scammer pretends to be someone they're not — or when an actor mimics someone in order to entertain.
Passwords	In life, reuse and recycle, except for passwords. Always create a different one for each of your online accounts.
Two-factor authentication	Two-factor authentication adds a second layer of security to your account with something you know (your password) and something you have (your phone).
Antivirus	It helps protect your computer against malware.
https	When shopping online, verify that the web address starts with https before entering your payment details. The 's' in https stands for secure.
Encryption	A form of encoding used by some email providers and websites to prevent others from snooping on your information.
Personal	This type of information shouldn't be shared online; it includes ID numbers, passwords and your home address.
Spam	Undesired or unsolicited emails or messages, usually sent out to a large number of users.
Symbol	A strong password will contain at least one: e.g.: ~ ! @ # $ % ^ & *
Security keys	Electronic tokens that can be used in addition to your password to access your online account.

Topic Sharing Online

Term	Definition
Oversharing	Revealing too much personal information about yourself.
Settings	You may want to adjust these to decide what you share and who you share it with.
Public	Information about you that is visible to everyone.
Private	Information about you that is only visible to you.
Privacy	The ability to selectively choose how much information you reveal about yourself.
Guidelines	Community rules that help keep social networks and other sharing websites fun and enjoyable for everyone.
Report	An action that you can take when you see something inappropriate on social media sites that you want to flag for review.
Block	An action that you can take to avoid interacting with obnoxious users on social media sites.
Reputation	People's perception of you, both online and offline.
Viral	When a picture, video or post is circulated rapidly on the web, it is said to have gone viral.
Digital footprint	Everything on the web that's about you, including photos, videos, mentions and more.
Geolocation	The estimation of the geographical location of a mobile phone or a computer connected to the Internet.
Profile	Information about someone on a website that includes name, picture and/or other details.
Avatar	A graphical representation that some people use on their social network profile instead of a real picture.
Upstander	A person who speaks up and takes action when they see someone being treated unfairly online — the opposite of bystander.
Cyberbullying	The use of social media and other electronic means to harass or intimidate a person.

Protect Your Online Accounts

Your online accounts enable you to share information with family and friends, such as photos and videos from last week's family get-together. Your online accounts also allow you to do common transactions from your home, such as transferring money, paying your bills or shopping for different products.

Because online accounts are tied to our online identity, it's important to take steps to protect them from intrusion with a strong password.

Setting a Strong Password

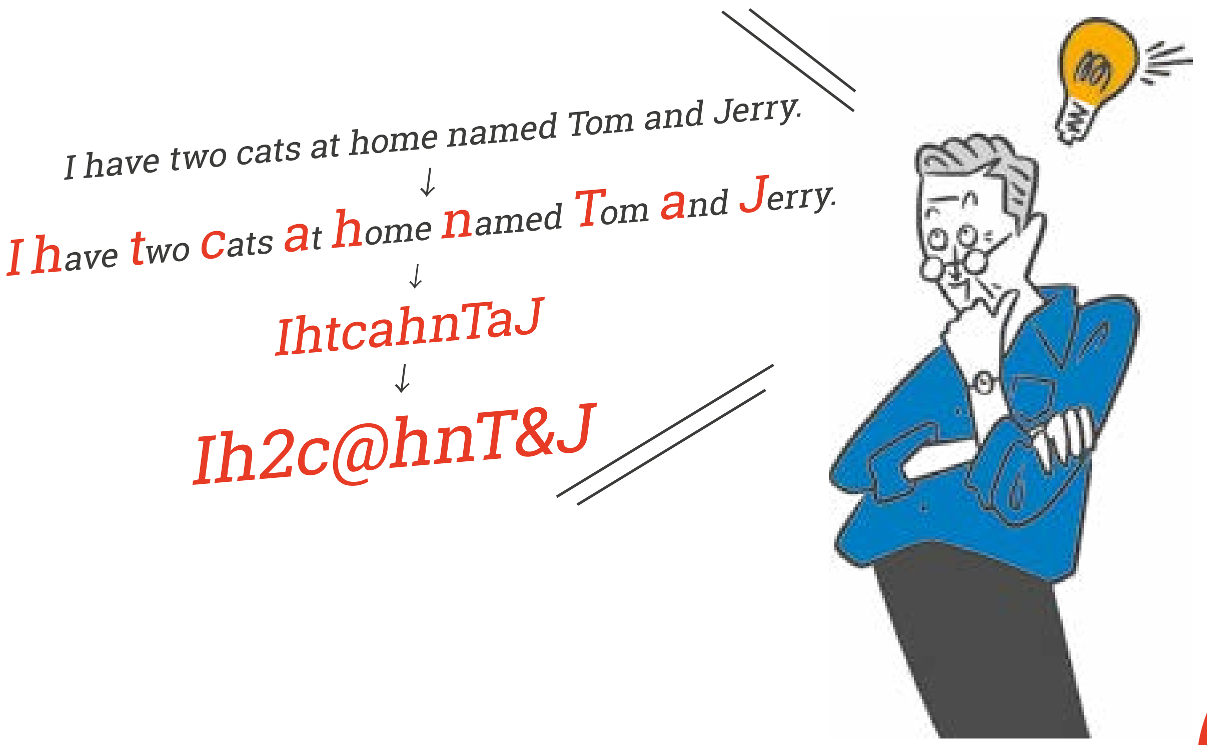
A strong password is the first line of defence against people who want to break in to your account to access your personal information.

These are some of the key attributes that make a password strong:

- Length: make your password at least 8-9 characters long.
- Mix of characters: use a combination of lowercase and uppercase letters, numbers and symbols.
- Avoid using personal information, like your birthday or your child's name.

Let's look at how you can create your own strong password.

- Think of an easy-to-remember sentence. For example, I have two cats at home named Tom and Jerry.
- Now take the first letter of each word using lowercase and uppercase letters where appropriate. That should give you **IhtcahnTaJ**
- Where possible, replace letters with numbers or symbols: **Ih2c@hnT&J**


I have two cats at home named Tom and Jerry.
↓
I have two Cats at home named Tom and Jerry.
↓
IhtcahnTaJ
↓
Ih2c@hnT&J

Using Unique Passwords

Now that you have a strong, easy-to-remember password, it may be tempting to use it for all of your online accounts. However, reusing passwords is risky. If someone finds out the password for one of your online accounts, like your email, they could also get access to all of your other accounts, including your online banking and shopping accounts. That's why it's important to create a unique password for each of your online accounts.

But what can you do to make it easier to remember multiple passwords? In addition to creating your passwords using an easy-to-remember sentence, you can also use a password manager like passwords.google.com.

Account Recovery

Everyone forgets their password at some point. Fortunately, most online services give you the option of adding a recovery phone number or secondary email address so that you can receive instructions on how to regain access to your account should you forget your password. To make sure that you can get back into your online accounts quickly and easily, make sure to set up password recovery options before that happens!

Other Tools

Would you like to review and update the security settings for your Google account? You can go to myaccount.google.com and do the Security Check-up to see what devices you've used to log in to your Google Account, and take additional steps to secure your account, such as adding 2-Step Verification (g.co/2step).

Exercise Care When You Share

The Internet has revolutionised how people communicate with each other — you can now reach people near and far with just one click. While it's exciting to share pictures, memories and ideas, it's important to exercise care, and to ensure that you only share personal information with people that you trust.

Remember that anything you share online — whether on social media, online forums or instant messaging apps – could reach more people than you intended at the time of sharing, if sent to the wrong party.

So before you hit send, know **what** you are sharing, **who** you are sharing it with and, most importantly, **why** you're sharing it — do they really need to know?

Know What You Share

In addition to setting your own boundaries around what you want to share, it's important to be cautious with sensitive information. For example, if you are at a party, you may be comfortable sharing your name with a new acquaintance upon introduction, but it is unlikely that you would share your home address with someone you just met. In the same way, it is essential to treat sensitive information with care when sharing online.

Examples of sensitive information may include:

- **Your full name and email address.** While you may need to share this information with people you know, it may be wise to refrain from posting your full name and email address on public forums or online spaces.

- **Photos of yourself, or of family and friends.** Photos may sometimes reveal more information than you intended. For example, a family photo with your house in the background could reveal where you live.

  Moreover, photos taken with a mobile phone or device may contain the coordinates of where the photo was taken (this is often referred to as geotags). This information could be useful to help you remember where you took a photo, but should be removed if you do not wish to share location information with others. Check the settings on your phone's camera to turn geotagging on or off.

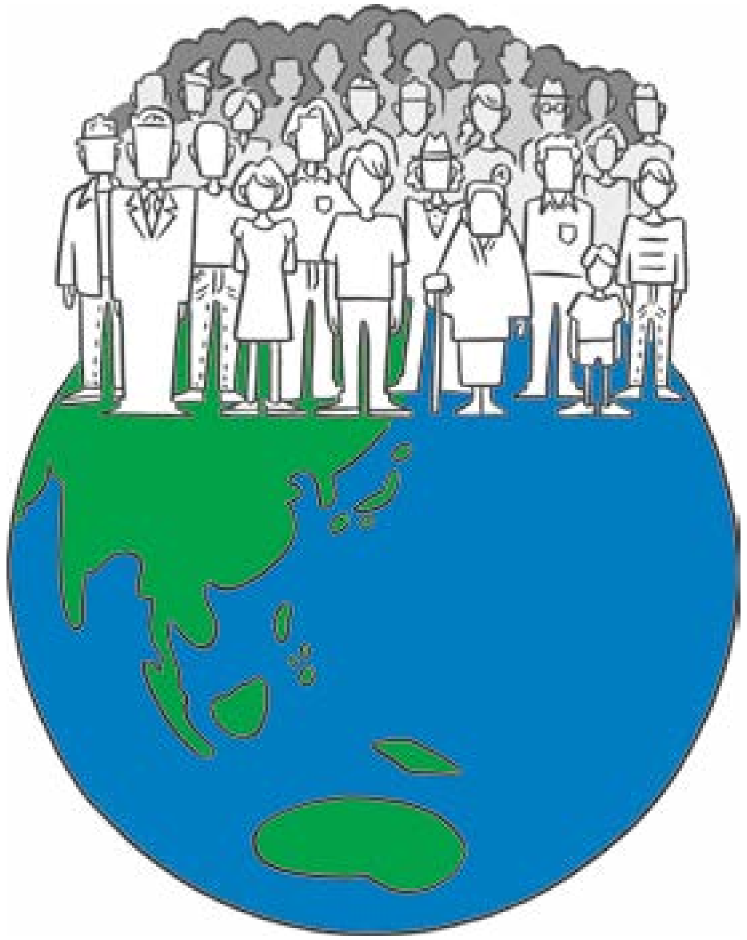
- **Your bank account information, PIN or password.** This is extremely sensitive information, and should not be shared online with others. The only time that you should type in this information is when you directly access your bank's official website or app. To avoid online scams, don't click on links to your bank or other websites if they're sent to you via email or text message. Instead, go directly to the site by typing the web address into your browser's address bar.

Know Who You Are Sharing With, and Why

How sensitive information is depends in part on who you intend to share it with. For example, you may want to share photos from last week's family outing only with family and close friends, while you may want to write an honest restaurant review on a business review website for everyone to read.

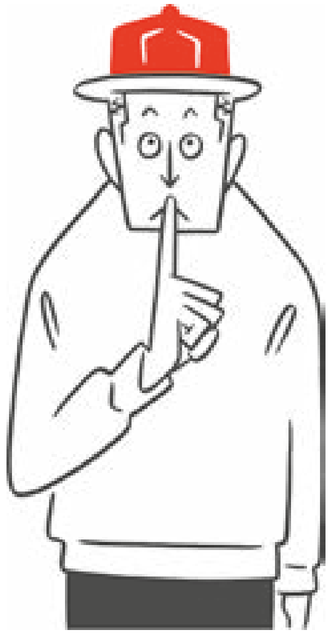
In order to better understand with what audience you may want to share different types of information, it's good to know the sharing options available on most social media sites:

1. **Share publicly or with everyone:** this option means that everyone can see what you post. For example, many people share film, restaurant and product reviews publicly to help others decide what film to watch, where to eat or whether to buy a specific product.



2. **Share only with specific people:** this option means that only some people can see what you post. Examples of content that you may only want to share with specific people include family photos and videos. It's important to remember that the people you share content with could reshare it with others.

3. **Post privately:** some websites or social networks allow you to upload photos and other files privately for your own viewing.



Identify and Avoid Scams

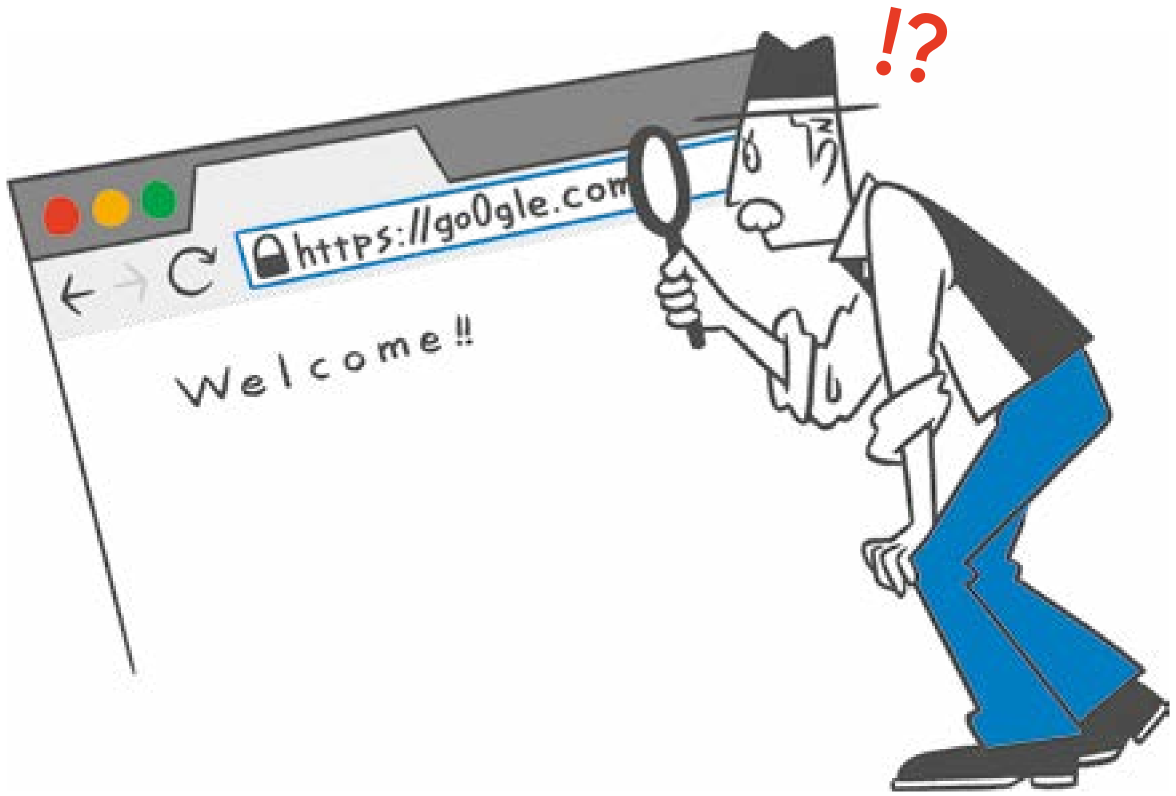
Most of the content you find online is good and can be useful, but just as in the offline world, you also need to watch out for the occasional bandit. Online scammers use different techniques to trick people into revealing their personal information and financial details. Here are some tips to help you avoid online scams.

Pause Before You Post

Always pause and evaluate carefully all online requests for action or personal information. This gives you time to think and act wisely rather than react.

- Think twice before sending personal information to someone online. This includes information such as your username and passwords. Remember that legitimate companies will never ask you to share your password over phone, email, text message or social media.

- Exercise care when using online banking, transfering money or making payments. Double-check the web address to make sure that it's correct. Scammers can make websites look similar to other sites that you use in order to steal your login information. To ensure a website is secure and encrypted, check that the web address starts with 'https' and not just 'http'.



Scammers will often use emotional manipulation techniques to get you to act before you have time to think, so be keenly aware of how you feel when you receive an email or text message asking you to do something specific, such as transferring money or calling a phone number. Scammers will try to make you feel:

- **A sense of urgency.** Be suspicious of special offers or prizes that seem too good to be true. Even though you may feel compelled to take advantage of the offer, it's important to pause and think. You may want to search online to check if other people have found the same offer to be a scam, or go to the official website to learn if the offer is actually true.

- **Fear.** Many scammers send fake warnings and virus alerts claiming that your computer or phone has been attacked or compromised. They will usually ask you to download software to fix it. Remember: a website or an ad cannot detect if your device has been infected. Software and apps should only be downloaded from reputable sources, such as the official app store on your phone.

  Similarly, some scammers may tell you that your online account has been compromised and that you need to change your password immediately to prevent further harm. Instead of reacting, remember to pause and check if the message is legitimate. If you are concerned, go directly to your account and change your password. Do not click on links in suspicious emails or text messages.

- **Anger or excitement.** Some scammers create articles with sensational titles that generate anger or excitement in order to drive views to their websites, where they make revenue through advertising. Don't share articles or other content if you believe it may contain inaccurate information.

- **Compassion or Adoration.** Some scammers may attempt to befriend you on social media sites. Be on your guard, especially when people you have recently met online profess their feelings for you; want to send you expensive gifts; or tell you they are experiencing hardship and need financial help from you.

  Remember: If you feel pressured to act quickly, do the opposite — pause, check on the request, and think twice before sending any personal information.

Discerning Between Legitimate and Dubious Information

We receive a lot of information every day through newspapers and television, as well as through websites, social media platforms or instant messages from friends. We often pass this information on to our family and friends. But just because something is online, it doesn't mean that it is true or reliable. You should always ask yourself these four questions:

1. **Where** was this content originally published? Is it from a reputable source? Is the website seeking to inform or entertain? To be sure that a piece of information is accurate, check at least 3 reputable sources.

2. **Who** wrote it? Can you identify the author? Are they qualified to speak or write on the subject?

3. **What** is the viewpoint of the message or article? Is the information presented in a balanced way? Could the author be biased in some way?

4. **When** was the article written? Is the information up-to-date and relevant?

Crossword Puzzle

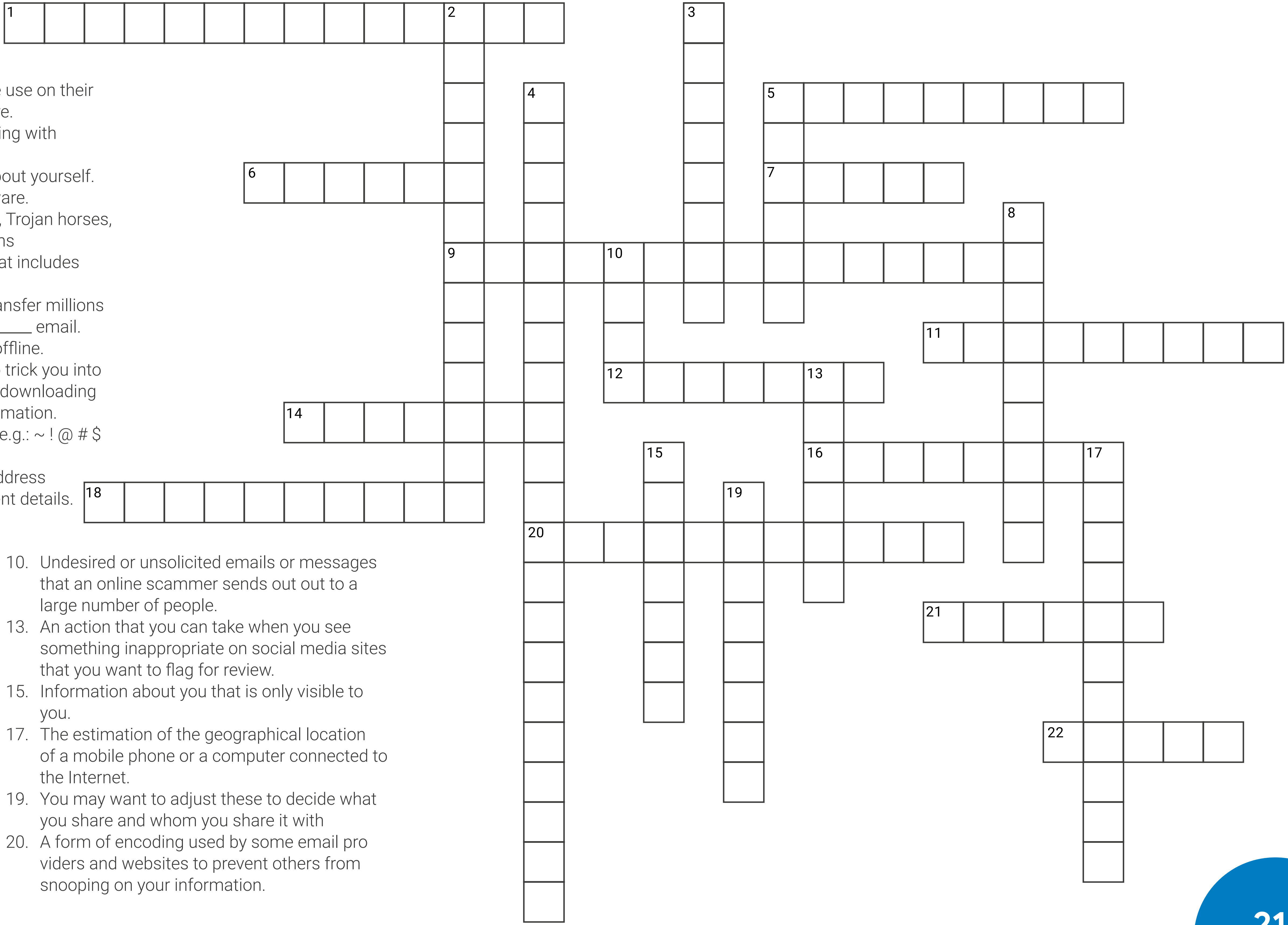
For answers, check Terms Worth Knowing starting on page 5.

Across

1. Two-factor ______ adds a second layer of security to your account with something you know (your password) and something you have (your phone).
5. In life, reuse and recycle, except for passwords. Always create a different one for each of your online accounts.
6. A graphical representation that some people use on their social network profile instead of a real picture.
7. An action that you can take to avoid interacting with obnoxious users on social media sites.
9. Revealing too much personal information about yourself.
11. It helps protect your computer against malware.
12. A term that encompasses computer viruses, Trojan horses, worms, adware and other malicious programs
14. Information about someone on a website that includes name, picture, and/or other details.
16. Remember the rich prince who wanted to transfer millions of dollars to your account? Well, that was a _____ email.
18. People's perception of you, both online and offline.
20. Social _____ happens when someone tries to trick you into doing something dangerous online, such as downloading malicious software or sharing personal information.
21. A strong password will contain at least one: e.g.: ~ ! @ # $ % ^ & *
22. When shopping online, verify that the web address starts with _____ before entering your payment details.

Down

2. When an online scammer pretends to be someone they're not — or when an actor mimics someone in order to entertain.
3. This type of information shouldn't be shared online; it includes ID numbers, passwords and your home address.
4. Following community _____ help keep social networks and other sharing websites fun and enjoyable for everyone
5. Information about you that is visible to everyone
8. Your digital _____ is everything on the web that's about you, including photos, videos, mentions and more.
10. Undesired or unsolicited emails or messages that an online scammer sends out out to a large number of people.
13. An action that you can take when you see something inappropriate on social media sites that you want to flag for review.
15. Information about you that is only visible to you.
17. The estimation of the geographical location of a mobile phone or a computer connected to the Internet.
19. You may want to adjust these to decide what you share and whom you share it with
20. A form of encoding used by some email pro viders and websites to prevent others from snooping on your information.



Online Safety Guide for Seniors