AARP Fraud Watch Network

Fraud Watch Overview

Sept 2024

Identify and Protect

Agenda

- Warning signs of fraud and recognizing vulnerabilities
- Advice on protecting yourself
- Identify resources to report and resolve problems

FTC Report on top Scams

Fraudsters tricked roughly 690,000 people in 2023 into giving them money during a scam, resulting in total losses of $10.02 billion, according to the FTC.

Top Scams Reported	Total Losses
1. Imposter Scams	$450 million
2. Online Shopping	$250 million
3. Business Email	$200 million
4. Romance Scams	$150 million
5. Identity Theft	$100 million

Warning Signs

Why are scammers able to steal from us?

- They play on our emotions!
  - Fear
  - Excitement
  - Desire for romance

- Examples:
  - “Your Social Security account has been frozen”
  - “Your computer has a dangerous virus”
  - “I never thought I could love someone like I love you”

New 2023: AI Voice Scams

"Biden Audio Deepfake Alarms Experts in Lead-Up to Elections"

- Scammers use AI technology and audio data collected online to clone a voice
  - Convince a victim that a loved one needs immediate financial assistance.

- **Warning Signs:**
  - Only briefly hearing voice
  - Can not answer questions
- **Advise: Never answer your phone**

How to protect yourself

- **Sleep on it.** Never respond same day to money or information request
- **Google It:** discussed as scam?
- Medicare and Police **will never call** you and ask for money or information
- Any request to send **Gift card** is a scam

A few simple protection rules

- Think before you post
- Create a powerful password.
- Protect your PC.
- Manage your digital reputation.

This is Cybersecurity

How to protect yourself

Ransomware:
Illegally encrypting your computer data and charging you for a key to unlock it

- Ways to keep your computer systems safe
- Keep device software up-to-date
- Install Antivirus/Antispyware Software
- Turn off/sleep computer when not in use
- Backup data to cloud or external drive

What is Phishing?

Phishing /ˈfiSHiNG/

The attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a something trustworthy, like a bank.

Phishing example

Dear Heather,

Your Apple ID was used to sign in to iCloud on an iPhone.

Time: July 06, 2017
Operating System: iOS;10.0.1

If you recently signed in to this device, you can disregard this email. If you have not recently signed in to an iPhone with your Apple ID and believe someone may have accessed your account, please click here to confirm your details and change your password.

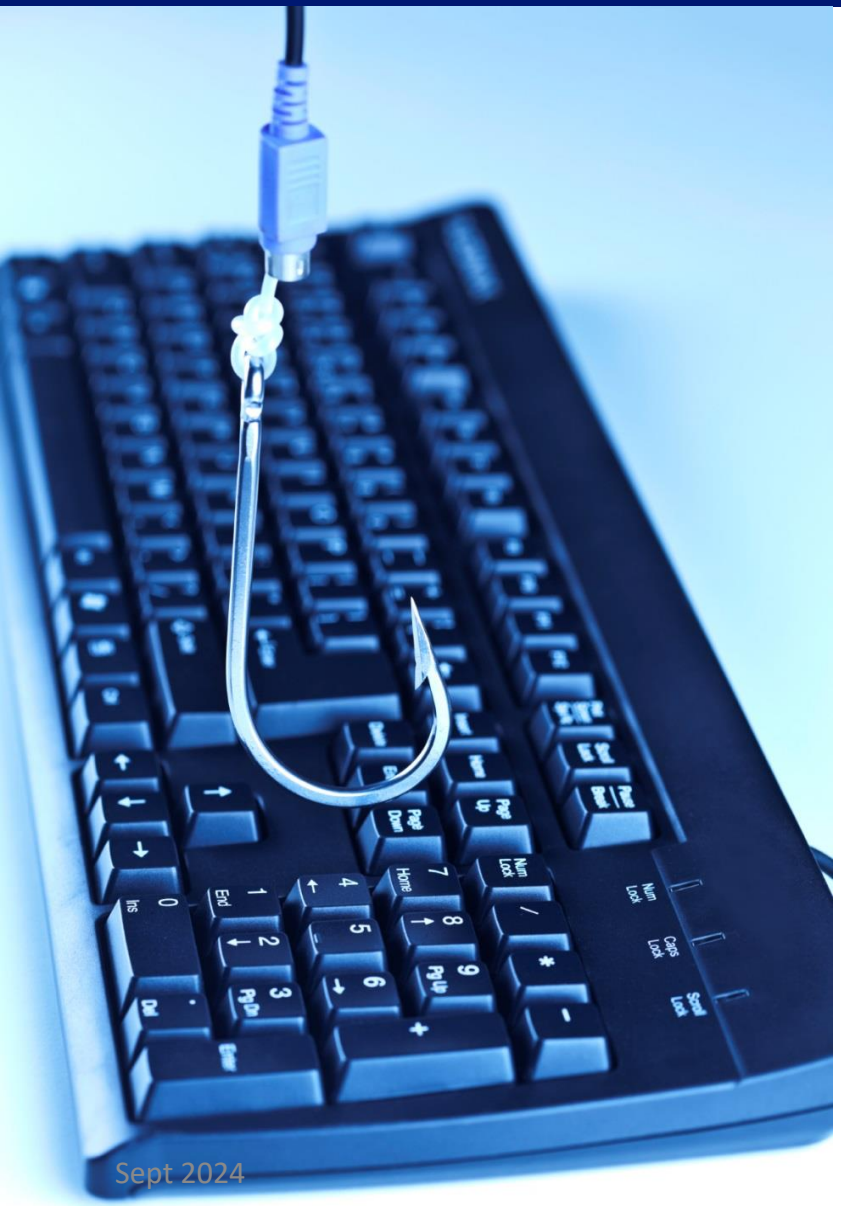
Apple Support
My Apple ID | Support | Privacy Policy | Copyright © 2014 iTunes

Apple Canada
7495 Birchmount Road
Markham, ON L3R 5G2. All rights reserved.

Go to Apple Canada for more information on our latest new products.

1. Looks legitimate
2. You are a Apple customer
3. Convincing detail
4. Convincing epilogue
5. Increased potential for users to click links provided without thinking

Protecting your eMail



- Don’t click on email **link**!
- Don’t open **files** from strangers
- Check **actual** email address
- Strange message from a friend? Be wary

Meta
Formerly: Facebook

- Facebook has a lot of benefits, but the challenge is to understand the risks of using it.

- Anything and everything you post can be linked to you, and can also affect other people

This holds true for all social media platforms

- Instagram, Youtube, TicToc, Twitter, Reddit

Facebook and GDPR

Facebook's Commitment & Preparation

- Data protection is central to the Facebook Companies (Facebook and Messenger, Instagram, Oculus and WhatsApp).

- We comply with current EU data protection law, which includes the GDPR.

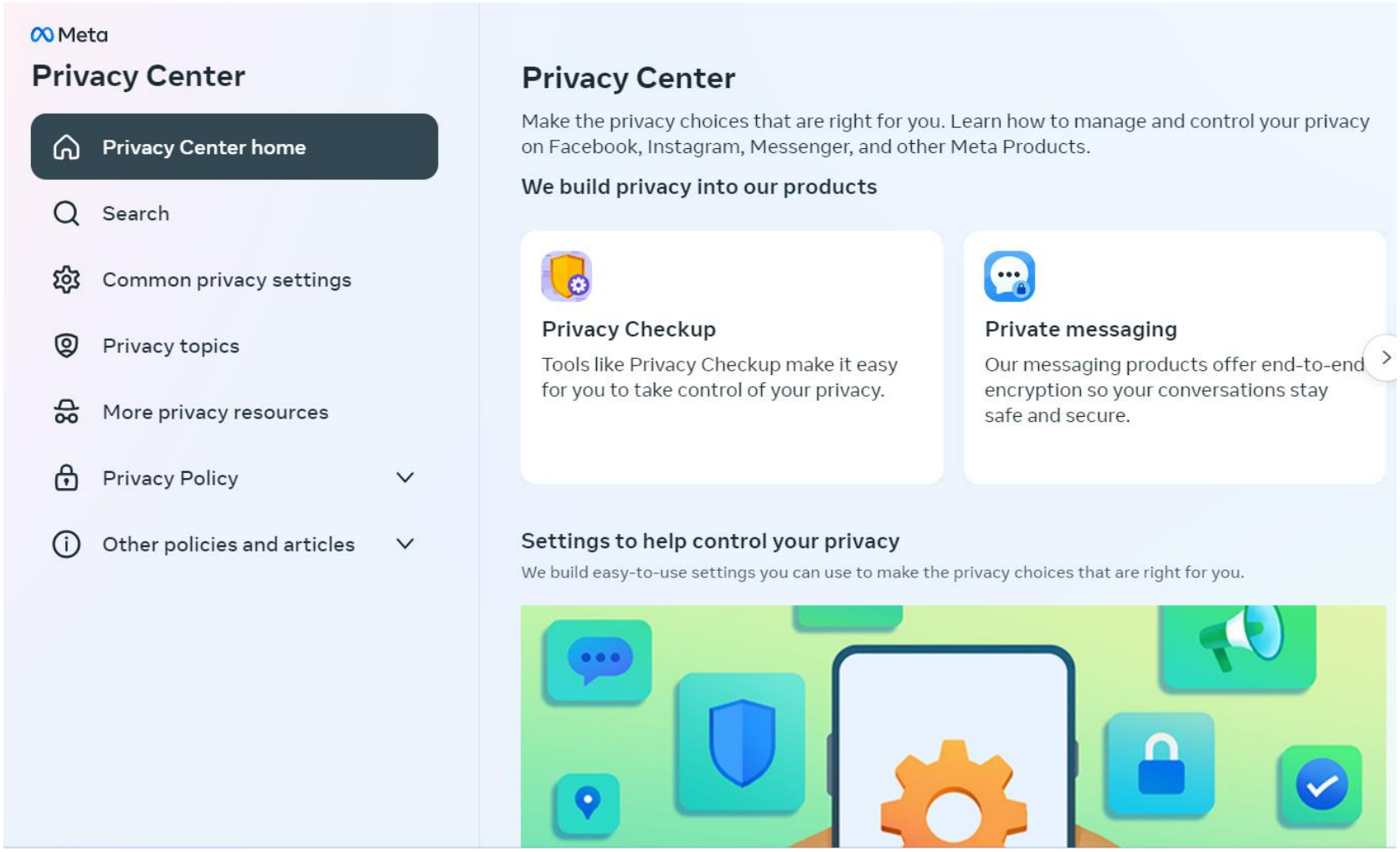
- Our GDPR preparations were led by our Dublin-based data protection team and supported by the largest cross-functional team in Facebook's history.

Your digital reputation – and Facebook

- Who are my friends?
- What do I allow my friends to see?
- What do people who are not my friends see?
- What does my wall say about me?
- How do I present myself when I write on my friends' walls?
- Does every photo of me represent me positively?

Make sure to review your privacy settings!

Facebook Privacy Center



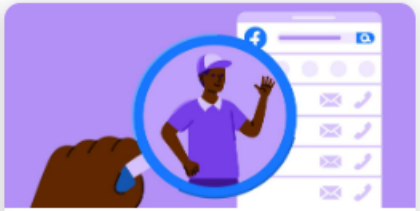
Facebook Privacy Checkup

Privacy checkup

We'll guide you through some settings so you can make the right choices for your account. What topic do you want to start with?

Who can see what you share

About 6 months ago



How people can find you on Facebook

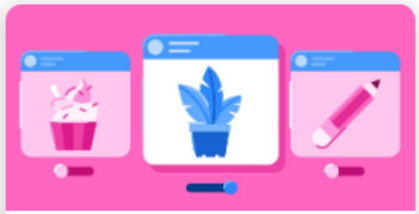
About 6 months ago

How to keep your account secure

About 6 months ago

Your data settings on Facebook

About 6 months ago

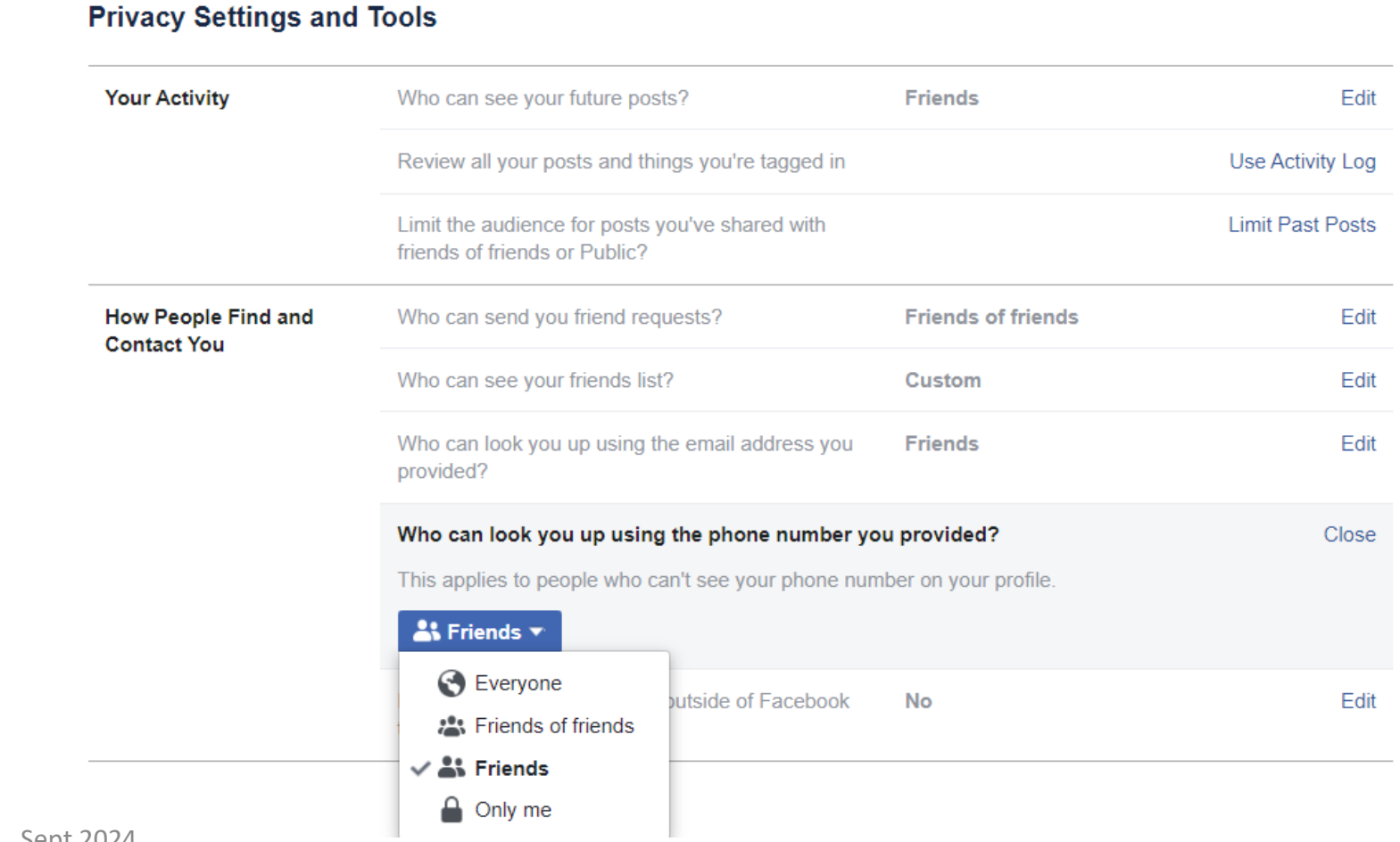


Your ad preferences on Facebook

About 6 months ago

Deciding who can see and communicate with you

Who can see your information, find you and communicate with you



Online ID Protection

Regularly Change Passwords

1. Create strong, easy to remember password/passphrase
   - *StageCoach1929$*

2. Use a Password Manager
   - *Example: Last Pass*

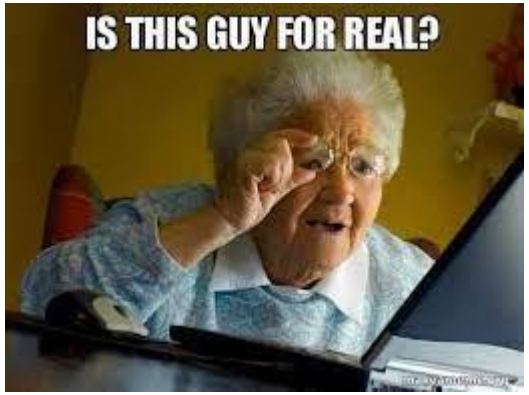
Add 2-factor authentication to websites
- **Cell Phone authentication code**

Summary: Tips to Remember

- Keep control of your data
- Passwords
  - Make them powerful
  - Keep them secret
  - Use different passwords for different sites
  - Change them periodically
- Protect your personal computer
- **Manage your digital reputation**
- Protect yourself, your data, and your friends
- Negative posts about other people reflect badly on you
- Be fair with other people's data
- Ask, if you are unsure

Fraud Prevention Tips

- **Stay informed:** Educate yourself
- **Verify identities**: Confirm the identity



- **Be cautious online**: Avoid clicking on suspicious links
- **Trust your instincts**: If something feels off or too good to be true, it probably is
- **Seek help**: Don't hesitate to reach out

If your Identity is Stolen

- Do not feel ashamed or embarrassed – you are a victim!
- Contact your financial firm/credit card fraud hotline
- Submit an FTC Identity Theft Report
  - *www.identitytheft.gov*
- File a police report with local department

- Notify other agencies such as IRS, Medicaid/Medicare Fraud Office, State AG

Where to report in NC, and get help

1-855-408-1212 Opt 1

1-855-408-1212 Opt 2

NORTH CAROLINA DEPARTMENT OF JUSTICE
OFFICE of the ATTORNEY GENERAL

Consumer Protection
(919) 716-6400

AARP®

Fraud Watch Network

aarp.org/fraudwatchnetwork

If you or someone you know has been a victim of fraud, contact:

877-908-3360