Safety and Security

Tom Davis – Technical Support Repair Shop

Nancy Nicholson - Communications

Agenda

Browser Security

Microsoft - Google

Bad Password Habits

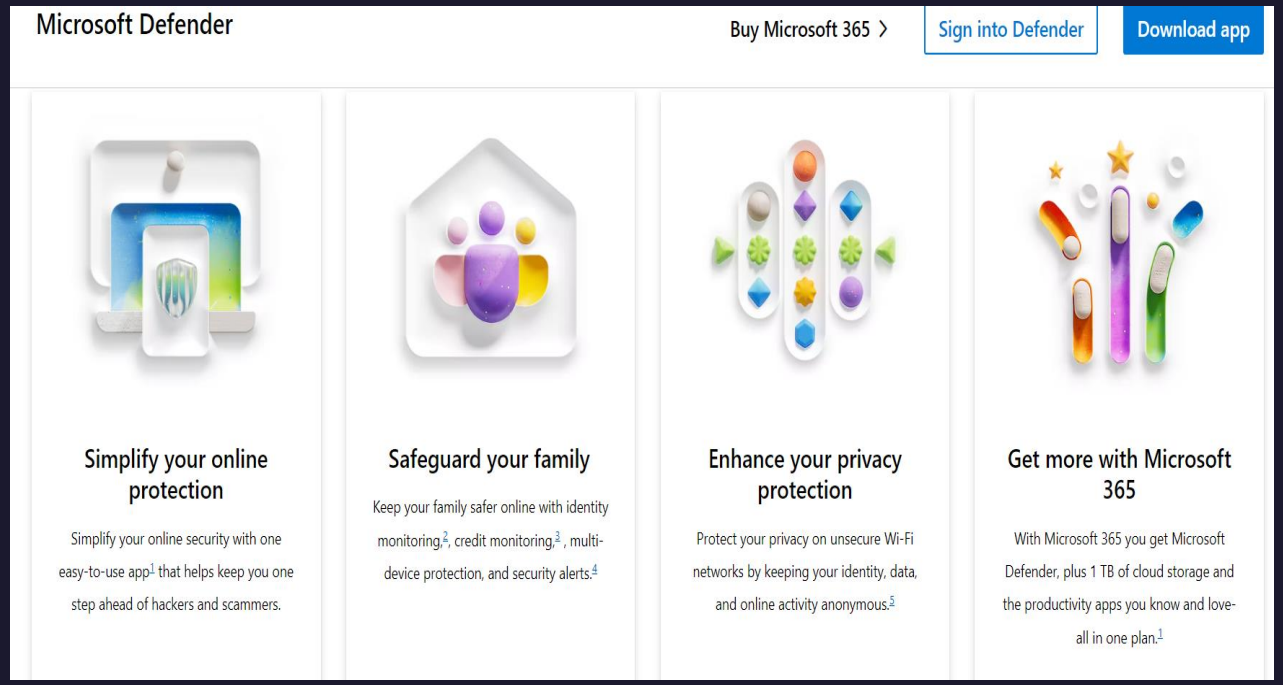
Delete Old Acconts

Remove Yourself from the Internet

Introduction

- The big push these days is for more security to protect us from the hackers that want to get our important information and use it for nefarious reasons.All of the big companies are continuously trying to thwart then from doing that.We must keep our devices updated.

BrowserSecurity Microsoft



All-in-one online protection

- **Manage your online security in one place**

. Check the security status of your family’s devices.
. Get timely alerts and notifications across your devices.
. Take recommended actions to improve your online security.
. Receive quick security tips to be safer online.
. View alerts and device activity history from the past 30 days.
. See the status of other antivirus protections you may be using, such as Norton or McAfee.
. Easily access your dashboard in the app or a web browser.

Experience trusted device protection for you and your family

- Protect your devices against new and existing threats with continuous antivirus and anti-phishing scans.[7]
- Get alerted if malicious apps are found and take steps to uninstall and remove the threats.
- Receive notifications across your devices when a security risk is identified.
- Specify apps and files you use regularly and don’t want Microsoft Defender to scan.

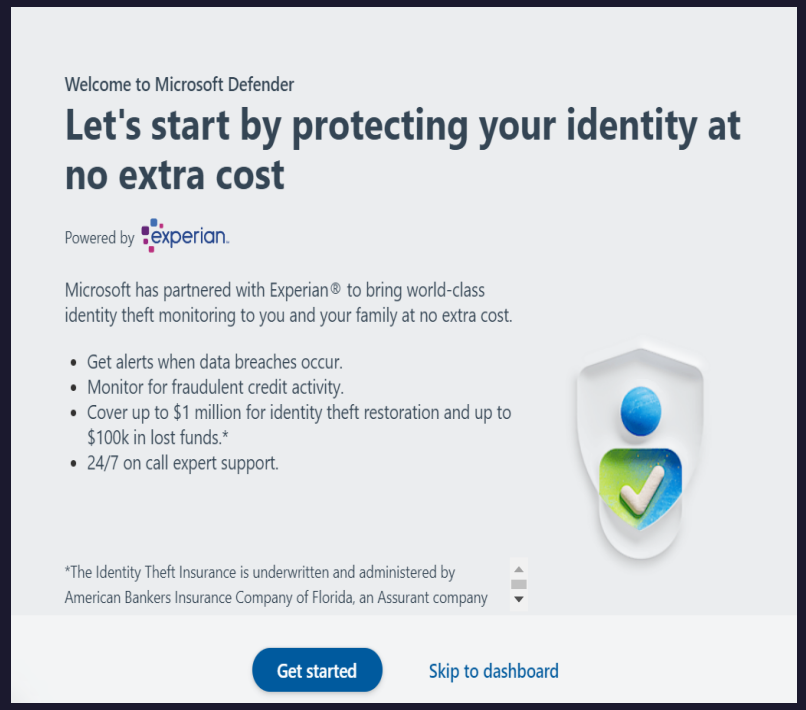
Experience trusted device protection for you and your family

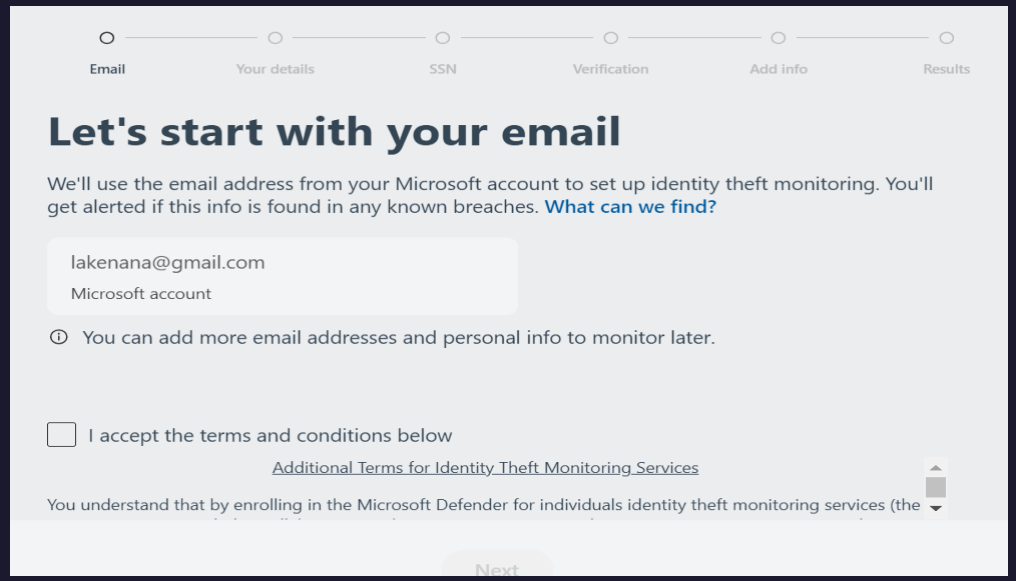
- Protect your devices against new and existing threats with continuous antivirus and anti-phishing scans.[7]
- Get alerted if malicious apps are found and take steps to uninstall and remove the threats.
- Receive notifications across your devices when a security risk is identified.
- Specify apps and files you use regularly and don’t want Microsoft Defender to scan.

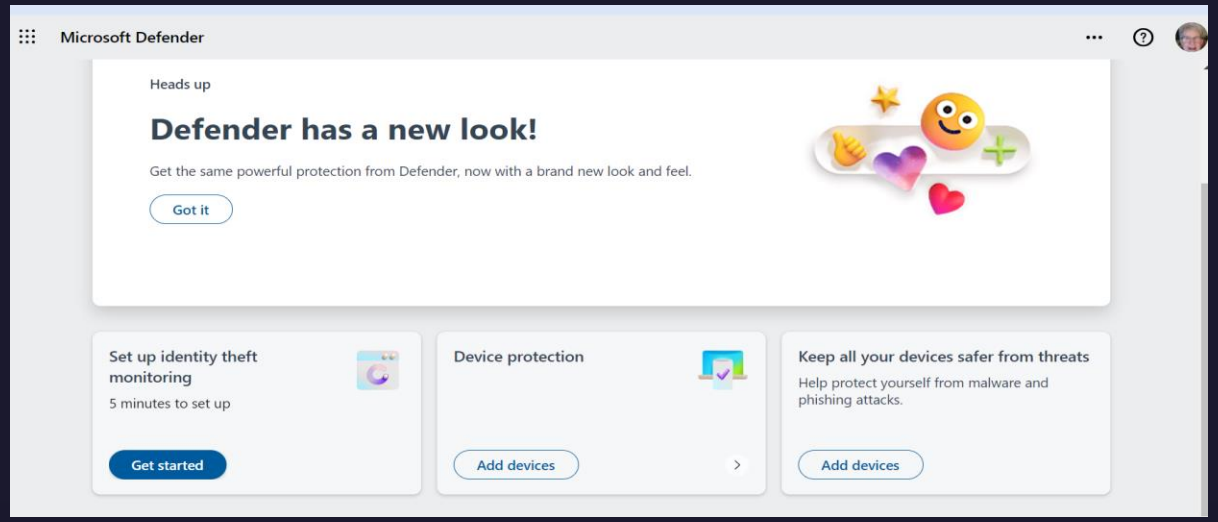
- ps are found and take steps to uninstall and remove the threats.
- Receive notifications across your devices when a security risk is identified.
- Specify apps and files you use regularly and don’t want Microsoft Defender to scan.

Keep your online activity safer from hackers and scammers

- Easily turn on a virtual private network (VPN) in your Defender dashboard at any time to safeguard your Wi-Fi connection.[5]
- Keep your location and IP address private with a VPN so hackers can’t trace your online activity.
- VPN keeps your traffic data encrypted to safeguard your identity.
- Get added protection with VPN when using bank account, credit card, and social security information while on an unsecure Wi-Fi.

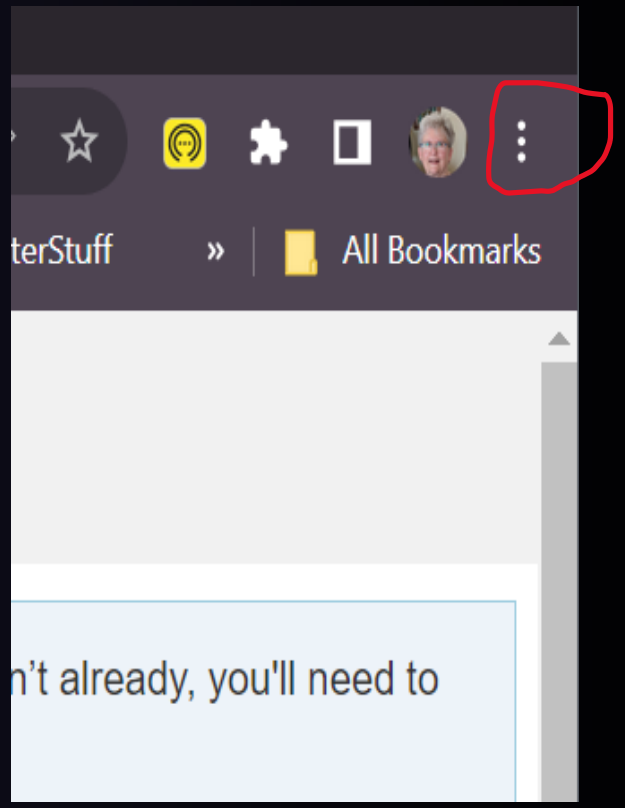

Welcome to Microsoft Defender
Let's start by protecting your identity at no extra cost
Powered by experian.
Microsoft has partnered with Experian® to bring world-class identity theft monitoring to you and your family at no extra cost.
• Get alerts when data breaches occur.
• Monitor for fraudulent credit activity.
• Cover up to $1 million for identity theft restoration and up to $100k in lost funds.*
• 24/7 on call expert support.
*The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company
Get started
Skip to dashboard


Email
Your details
SSN
Verification
Add info
Results
Let's start with your email
We'll use the email address from your Microsoft account to set up identity theft monitoring. You'll get alerted if this info is found in any known breaches. What can we find?
lakenana@gmail.com
Microsoft account
You can add more email addresses and personal info to monitor later.
I accept the terms and conditions below
Additional Terms for Identity Theft Monitoring Services
You understand that by enrolling in the Microsoft Defender for individuals identity theft monitoring services (the
Next

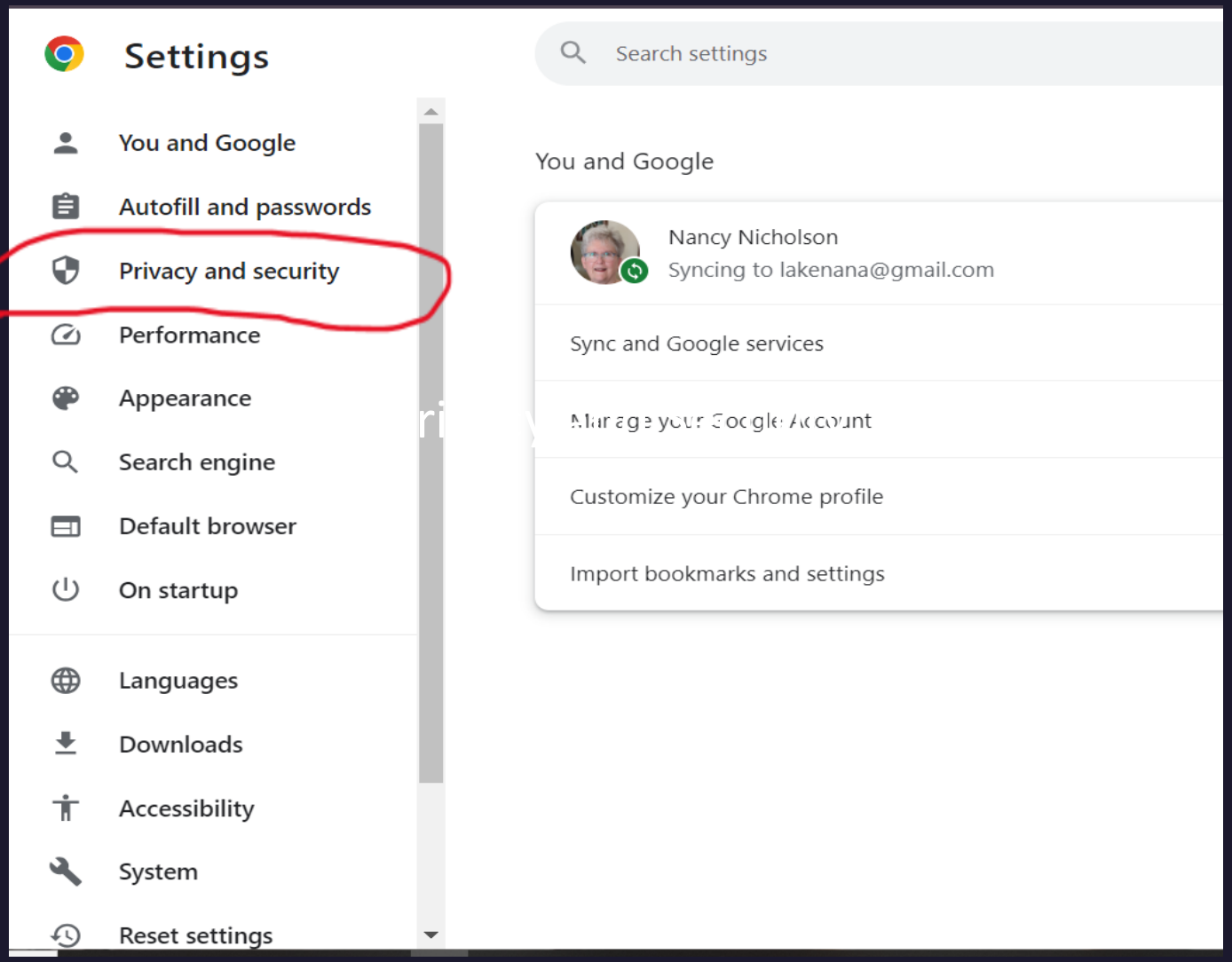

Microsoft Defender
Heads up
Defender has a new look!
Get the same powerful protection from Defender, now with a brand new look and feel.
Got it
Set up identity theft monitoring
5 minutes to set up
Get started
Device protection
Add devices
Keep all your devices safer from threats
Help protect yourself from malware and phishing attacks.
Add devices

BrowserSecurity Google

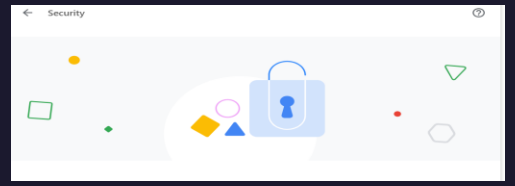
Google Browser – Check your Settings



Click the 3 dots ad then Settings in the pop-up Menu.


Settings
Search settings
You and Google
Autofill and passwords
Privacy and security
Performance
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
You and Google
Nancy Nicholson
Syncing to lakenana@gmail.com
Sync and Google services
Customize your Chrome profile
Import bookmarks and settings

Security



Safe Browsing

Enhanced protection: Faster, proactive protection against dangerous websites, downloads, and extensions.

Warns you about password breaches. Requires browsing data to be sent to Google.

Safe Browsing

- Predicts and warns you about dangerous events before they happen.
- Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in.
- Improves security for you and everyone on the web.
- Warns you if passwords are exposed in a data breach.
- Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.

- Warn you if passwords are exposed in a data breach
- **Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can’t be read by anyone, including Google.**
- nced
- **Always use secure connections**
- **Upgrade navigations to HTTPS and warn you before loading sites that don't support it**
- **Use secure DNS**
- **Determines how to connect to websites over a secure connection**
- **With your current service provider**
- **Secure DNS may not be available all the time**
- rn you if passwords are exposed in a data breachManage phones
- **Your devices**
- **You're signed into Chrome on these devices, so you can use them as security keys.**
- **Pixel 6a**
- **Linked devices**
- **Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can’t be read by anyone, including Google.**
- Advanced

Advanced you if exposed in a data breach

Always use secure connections

Upgrade navigations to HTTPS and warn you before loading sites that don't support it
Use secure DNS

Determines how to connect to websites over a secure connection
With your current service provider

Secure DNS may not be available all the time
Manage phones

Your devices

Manage phones

- You Manage phones
  Your devices
  You're signed into Chrome on these devices, so you can use them as security keys.
  Pixel 6a
  Linked devices
  devices
  You're signed into Chrome on these devices, so you can use them as security keys.
  Pixel 6a
  Linked devices

You can purchase a Google Titan SecurityKey, or use any FIDO compliant security key to enroll. We recommend two – one as your main key the other as your backup key.

- **Helping to make elections safer.**
- To make political organizations safer with Advanced Protection, we're partnered with Defending Digital Campaigns to provide free Titan Security Keys. See if your team is eligible for free keys.
  - Safe Guarding Human Rights

We have partnered with the International Foundation for Electoral Systems on global educational security for at risk groups so those who work to safeguard human rights can stay safe online.

Bad Password Habits

- 10 Bad Password Habits You Need to Break
- 10 Bad Habits you need to Break
  - Putting Personal information into Passwords
  - Using a “Keyboard Walking” Password
  - Reusing the Same Passwords Everywhere
  - Insecure Password Storage
  - Not Using a Password Generator or Manager
  - Skipping Multi-Factor Authetication
  - Never Updating Old Passwords
  - Using Passwords Instead of Passkeys

Delete your Old OnLine Accounts

- Close old accounts to protect your personal data, identity details, and credit card numbers from potential attackers or data breaches. You can check if an password has been leaked at haveibeenpwned.com.
-
- Use password managers or search through your email to find old accounts you no longer use.
-
- If you can't delete an account, remove financial and personal information, and consider anonymizing the account by changing the email address and personal details to something random to minimize the risk of data compromise.

The Best Way to Remove Yourself From the Internet

- Uninstall Unnecessary Apps
- Uninstall Unnecessary Apps
- Update or Delete Social Media Profiles
- Use a Data Removal Service

Make your Presence on the Internet Safe

Summary Questions

Thank You

Tom Davis

Nancy Nicholson

https://lakegastoncc.org