

Tech Safety

Anti-virus:

What is anti-virus software?

- Software to prevent attacks/ viruses
- Prevents, scans, detects, and deletes viruses
- Scans for files on computer and incoming files
- Some services include a VPN, firewall, and phishing protection
- Can block unauthorized websites to avoid being expose to threats
- Protects passwords

Paid options:

Deals as of July 2022

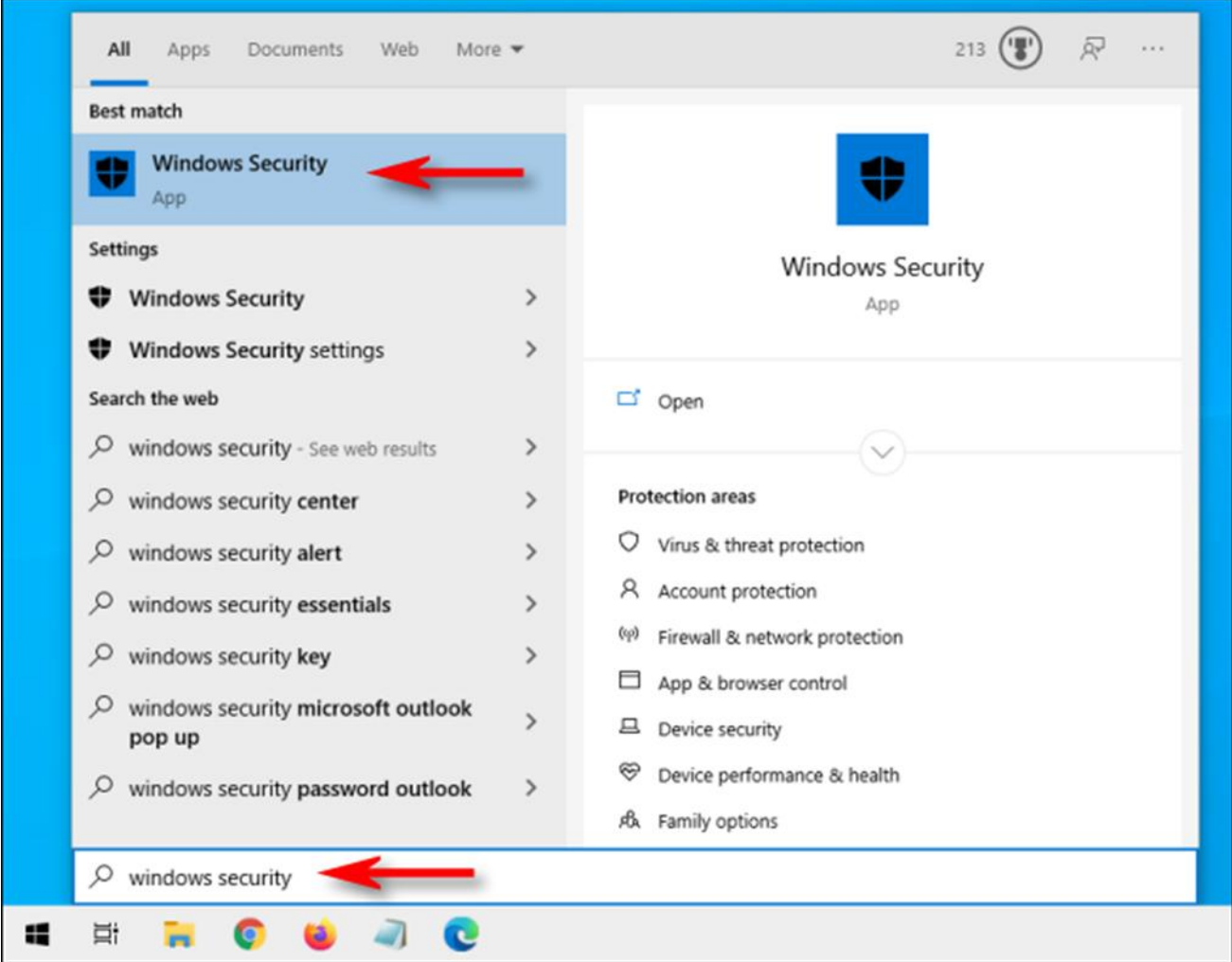
- \$19.99 1st year -[Norton Software for 2022 | Norton Products and Services](#)
- \$23.99 1st year-[Discover Bitdefender Identity Theft Protection](#)
- %23.99 1st year-[The next-gen antivirus protection for all your devices - Panda Security](#)

FREE- Windows Defender features:

- Virus and threat detection
 - Quick scan/ scan options
- Firewall and network protections
- App and browser control
- Device security/performance



How to scan with Windows Security:





Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
No action needed.



Account protection
No action needed.



Firewall & network protection
No action needed.



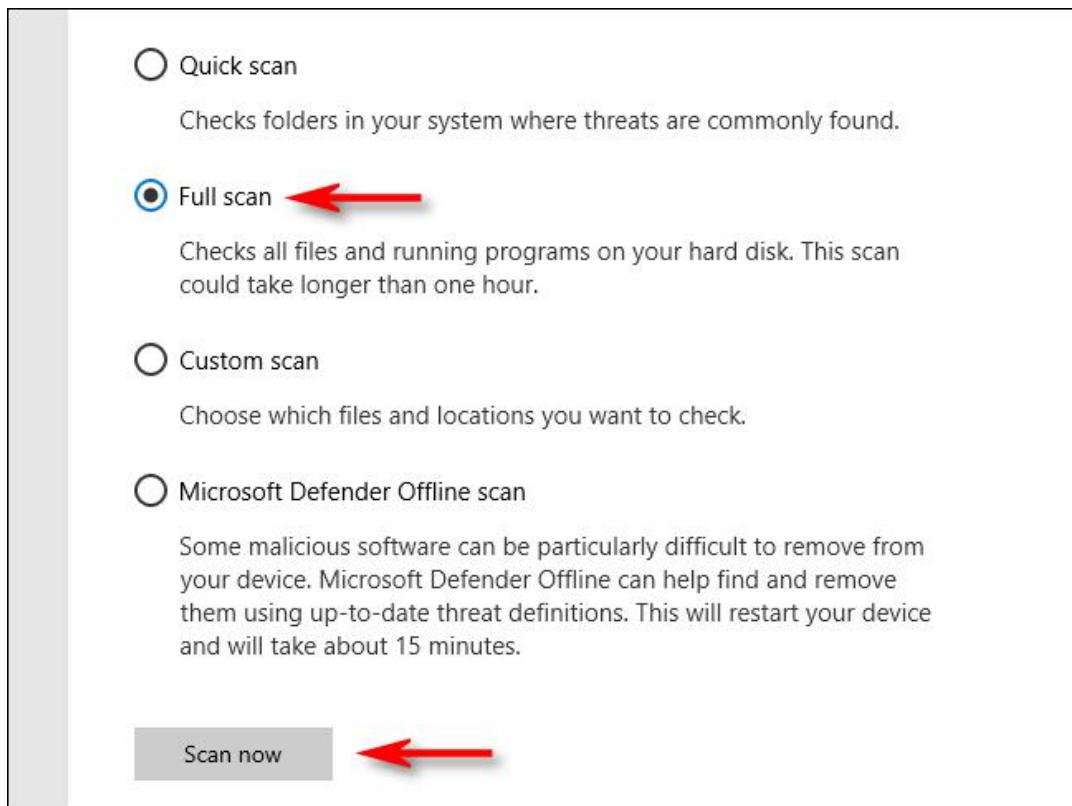
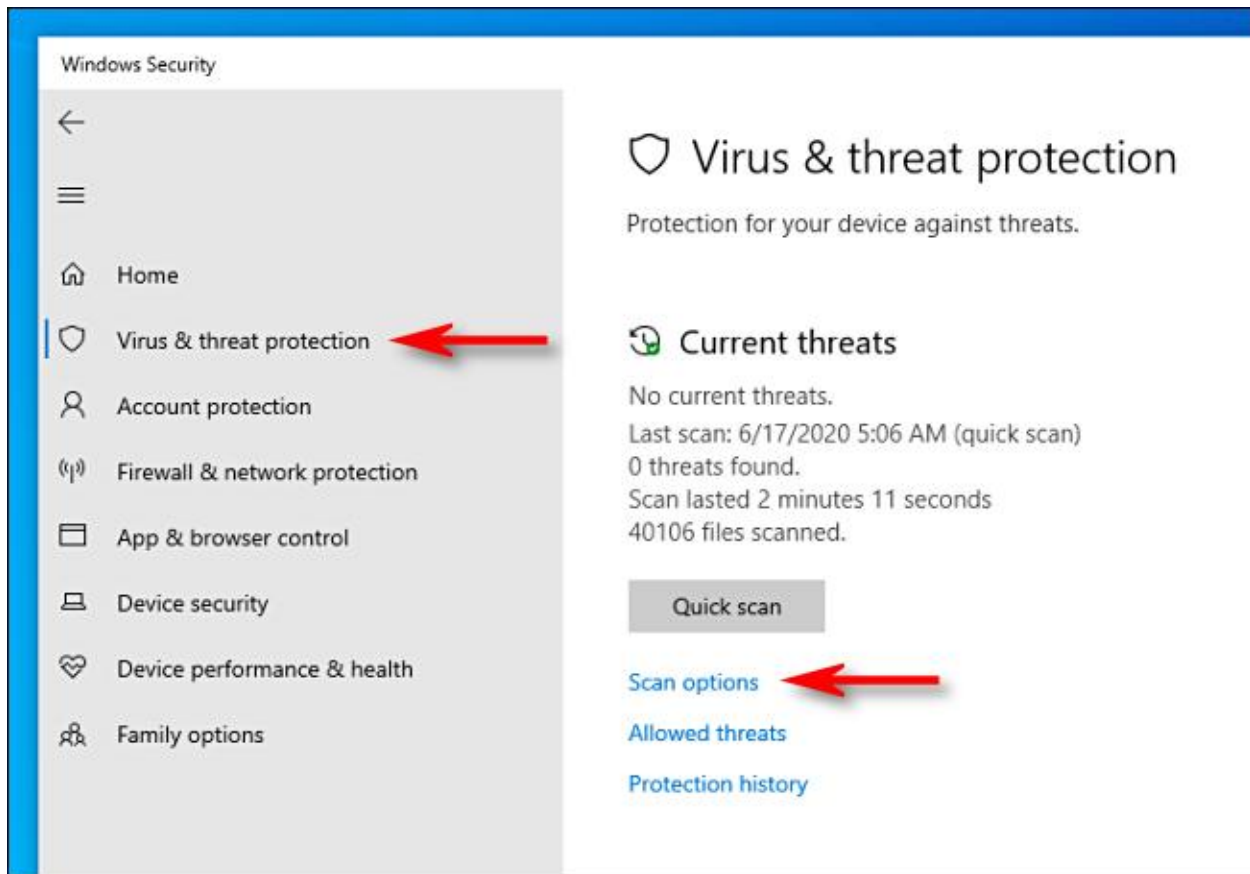
App & browser control
The setting to block potentially unwanted apps is turned off.



Device security
View status and manage hardware security features.



Device performance & health



Scan options

Run a quick, full, custom, or Microsoft Defender Offline scan.

Full scan running...

Estimated time remaining: 00:06:52

798475 files scanned

Cancel

Feel free to keep working while we scan your device.

[Protection history](#)

Current threats

No current threats.

Last scan: 6/25/2020 10:51 AM (quick scan)

0 threats found.

Scan lasted 37 seconds

35844 files scanned.

Threats found. Start the recommended actions.

Virus:DOS/EICAR_Test_File

6/25/2020 1:32 PM (Active)

Severe

Start actions



Safe Practices:

- Email:
 - Phishing- Individuals pose as an institution to get users to provide sensitive info
 - Look for spelling/grammar errors
 - Never open links/attachments from unknown emails
 - Never login to websites from an email link
 - Always go to a company's website to get into account/ for a phone number
 - Every month around 1.5 million new phishing sites are set up.
 - Be skeptical if there is a sense of urgency

Examples of phishing:

From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM



Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

Google



Gmail



Important: Your Password will expire in 1 day(s)



Inbox x



 MyUniversity

12:18 PM (50 minutes ago)



to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.

Please follow the link below to update your password

myuniversity.edu/renewal



Thank you
MyUniversity Network Security Staff

Sent: Monday, May 09, 2016 10:07 AM

To:

Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

1

We will process your request within 24 hours.

2

All features associated with your account will be lost.

To retain your account, kindly Cancel Request to continue using our services

[CANCEL REQUEST IMMEDIATELY](#)

3

Thank You,
Account Team

<http://bit.ly/1WTXQzB>

Please do not reply to this message. Mail sent to this address cannot be answered.

4

Browsing:

- Browsing:
 - Only shop from reputable websites
 - Avoid sharing personal info to anyone
 - Be skeptical when any amount of money is involved
 - “In 2020, [people ages 50 and older lost a dizzying \\$1.8 billion](#) to online fraud.
 - Be knowledgeable on common scams
 - If skeptical of a scam, conduct a web search
 - Create strong passwords with numbers, characters, and letters
 - Avoid using the same password for everything

- Avoid accessing private information on a public network

Educate yourself on common scams:

[Common Scams and Frauds | USAGov](#)

Common scams include:

- Tech support scam: Criminals pose as technology support representatives and offer to fix non-existent computer issues. The scammers gain remote access to victims' devices and sensitive information.
- Grandparent scam: Criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need.
- Government impersonation scam: Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- Digital Kidnapping: Criminals either take over or threaten to take over your social media account and threaten to post inappropriate/damaging material and demand payment.
- Fake charities: Scammers take advantage of natural disasters/ catastrophes and appear to be a charity

Protect yourself from phishing- Microsoft: <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>

How to download Windows updates:

- Updates are important to avoid crashes, bugs, and keep tight security
- Some updates require you to restart your laptop to finish

Steps:

1. Select the **Start (Windows) button** from the bottom-left corner.



2. Go to **settings** (gear icon).



3. Select the **Update & Security** icon



4. Choose the **Windows Update** tab in the left sidebar (circular arrows)



5. Click the **Check for updates** button. If there is an available update, it will begin downloading automatically.





HOW IT WORKS

Tech support scams use scare tactics to trick you into contacting fake tech support services.

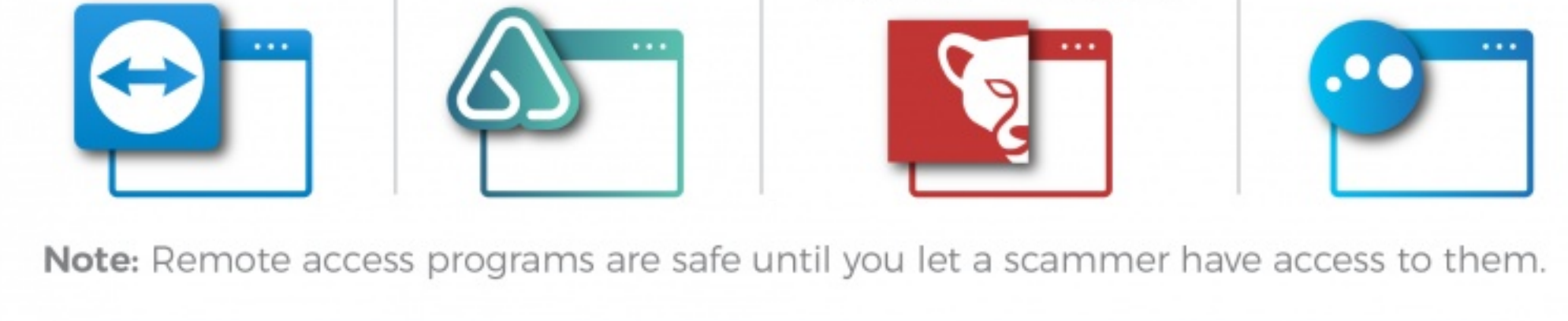
It usually starts with a pop-up...

Shows up in a browser tab

May imitate the blue screen error ...or an antivirus software

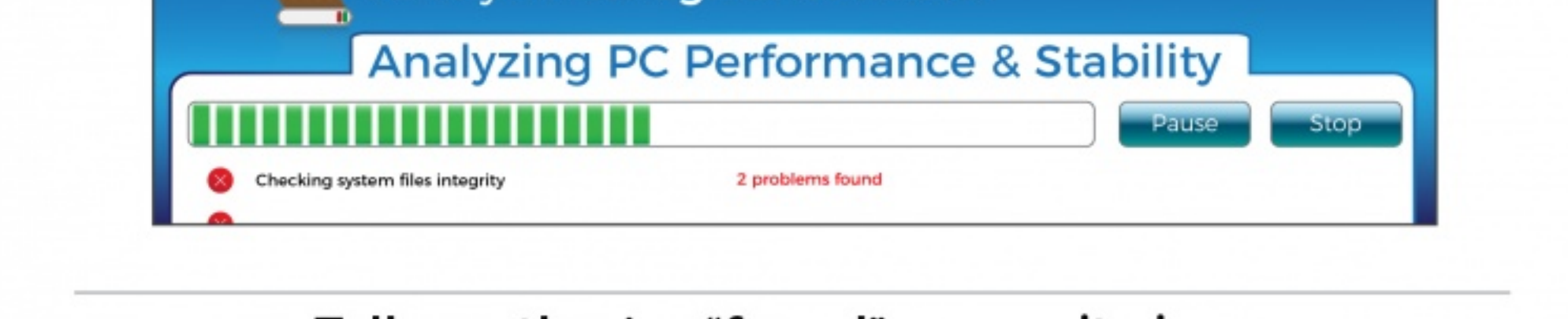
If you call the toll-free number the scammer may...

Ask you to download and install a remote access program such as:



Note: Remote access programs are safe until you let a scammer have access to them.

Then they'll "run" a diagnostic scan



Tell you they've "found" a security issue



Try to sell you a security service and ask you to pay a fee



WHAT TO DO IF YOU GET A POP-UP

- Don't click on anything.**
- Don't call the number listed.**
- Don't give any information out.**
- Power off your computer by holding the power button until it shuts off.**
- Wait at least two minutes before turning it back on.**

If pop-ups persist, contact TrioTel for help.

WHAT TO DO IF YOU'RE SCAMMED

- 1. Uninstall or turn off any remote management tools** you may have installed or turned on.
- 2. Get rid of malware.** Use antivirus software to clean your computer.
- 3. Change your passwords.** There's a chance your passwords may have been compromised.
- 4. Contact your credit card provider** to try reversing the charges. Also look over your statements for any charges you didn't make.
- 5. Monitor your identity.** The scammer might have accessed some of your personal information and may try using it elsewhere.
- 6. Unplug your computer and take it to a repair shop.** Have a professional look over your computer to make sure everything is in order.

Microsoft and Apple do not display pop-up warnings and ask you to call a toll-free number about viruses or security problems. They will never proactively reach out to you to provide unsolicited computer or technical support. Any communication they have with you will have had to be initiated by you.

Imposter Scams: Say No, Keep Your Dough

Imposter scams often begin with a call, text message, or email. The scams may vary, but work the same way – a scammer pretends to be someone you trust, often a government agent, family member, or someone who promises to fix your computer – to convince you to send them money or share personal information.

Scammers may ask you to wire money, put money on a gift card, or send cryptocurrency, knowing these types of payments can be hard to reverse.

According to the Federal Trade Commission, Americans lost more than \$667 million to imposter scams in 2019.

Learn to spot these scams and say no.




Recognize the Scam

You get a call, email or text message from someone claiming to be:



- A **FAMILY MEMBER** (or someone acting for them), saying your relative is sick, has been arrested or is in serious trouble and needs money right away.
- A **COURT OFFICIAL**, indicating that you failed to appear for jury duty and need to pay a fine or you will be arrested.
- The **POLICE**, saying you'll be arrested, fined or deported if you don't pay taxes or some other debt right away.
- From **SOCIAL SECURITY**, claiming that COVID-19-related office closures mean your benefits have been suspended.
- From the **IRS**, saying you owe back taxes, there's a problem with your return or they need to verify information.
- From your **BANK**, claiming they need to verify personal information before they can send you a new card.

Protect Yourself



Be Suspicious of any call from a government agency asking for money or information. Government agencies don't do that; scammers do.



Don't Trust Caller ID. Even if it might look like a real call, it can be faked.



Never pay with a gift card, wire transfer or cryptocurrency. If someone tells you to pay this way, it's a scam.



Check with the real agency, person or company. Don't use the phone number they give you. Look it up yourself. Then call to find out if they're trying to reach you—and why.

Report and Share

Tell your bank and be sure to share these tips with friends and family.

Learn more at ftc.gov/scamalerts and aba.com/consumers.



**FEDERAL TRADE
COMMISSION**



**ABA
FOUNDATION**