

Computer Security Results and Safety Guide

Bodell Bytes | Your Tech. Handled.

We checked your computer, made the agreed routine improvements, and practiced safer ways to respond to suspicious requests. Keep this results sheet and guide where you can find them.

Visit date _____

Your computer _____

Check	OK	Improved	Follow up	Not checked	N A
Windows update status	☐	☐	☐	☐	☐
Active antivirus protection	☐	☐	☐	☐	☐
Routine virus scan result	☐	☐	☐	☐	☐
Firewall protection	☐	☐	☐	☐	☐
Browser safety and notifications	☐	☐	☐	☐	☐
Unwanted software promotions	☐	☐	☐	☐	☐
Important account sign ins	☐	☐	☐	☐	☐
Recovery and screen lock	☐	☐	☐	☐	☐
Existing backup status	☐	☐	☐	☐	☐
Scam safety practice	☐	☐	☐	☐	☐

OK means checked today. Improved means changed today. Follow up means work remains. Not checked means no result. N A means not applicable.

Important findings and next steps _____

Pending updates or scan _____

Follow up owner and agreed date _____

These results describe the checks performed today. They do not guarantee prevention of every infection, account compromise or scam.

Questions about your visit? Call or text (989) 492-0058.
info@bodellbytes.com | www.bodellbytes.com

Everyday habits that help protect you

- Let Windows, your browser and antivirus receive supported updates. Restart when needed so an update can finish.
- Open a company's known app or saved bookmark to check an unexpected message. Do not use its login link, attachment, QR code or callback number to verify it.
- Treat urgent messages about payments, account trouble, delivery fees or refunds as a reason to pause. A logo, correct name, good spelling or secure-looking page does not prove the sender is genuine.
- Use a different strong password for each important account and the extra sign-in protection we discussed. Keep recovery information somewhere private.
- Never share a sign-in verification code, backup code or recovery code with someone who calls or messages you. Approve sign-in prompts only when you started signing in.
- Do not install software or grant remote access because an unexpected caller or pop-up tells you to. Contact help through a number you already know.
- Keep important files backed up using the arrangement you understand. Tell us if a backup is missing or failing; a security check does not automatically create one.

When an alarming pop up appears

Do not call its number, buy its offered fix or follow its instructions. Close the browser tab or window normally. If you cannot close it, stop using that page and contact known help. A genuine Microsoft warning does not contain a support phone number.

Antivirus promotions and browser notifications can look frightening. A message is not proof that a virus exists. Avoid hiding real security warnings just to stop the noise.

Guidance sources: FTC phishing and tech support scam guidance, and Microsoft tech support scam guidance. See the source links on the last page.

Recognize AI assisted scams

AI can help scammers produce convincing voices, writing, pictures and videos. You do not need to identify whether AI was used: verify the request independently before acting.

A familiar voice asks for urgent help

Even a voice that sounds like your child or grandchild can be copied. End the call and contact that person using a number you already know. If you cannot reach them, check with another trusted family contact. Do not use a number supplied by the caller.

An official sounding message demands action

A message may pretend to come from a bank, company or government office. Open the known official app or contact the organization independently. Do not transfer money to a “safe account,” hand cash or gold to a courier, or provide remote access because of a threat.

A convincing video promotes an opportunity

Celebrity and influencer endorsements can be fabricated. Pause and research independently before buying or investing. A realistic video or a promise of easy guaranteed returns is not proof.

Your response plan

Pause. End the conversation. Check through a known independent contact. Ask someone you trust before sending money or sharing information.

My trusted contact _____

Their known phone number _____

No secrecy or urgency rule should stop you from checking. Gift cards, cryptocurrency and unusual money-transfer demands are warning signs.

This page is based on FTC guidance about family impersonation, fake endorsements and other scams. It does not mean every scam uses AI or that software can stop every scam.

If you already clicked or shared something

- Clicked a link but entered nothing: close the suspicious page and seek known help if anything downloaded, installed or looks unusual. Clicking alone does not establish what happened.
- Entered a password or code: use a trusted device or official app to secure the affected account, change the password and review sign-ins. Contact the provider if access was lost. Do not keep interacting with the suspicious page.
- Allowed unknown remote access or installed software: stop the remote session and disconnect that computer from the internet. Contact known help; removing an app or one clean scan does not prove safety. Use another trusted device for urgent account protection.
- Sent money or disclosed bank/card details: promptly contact your bank, card issuer or payment provider using known details. Explain the scam and ask what can be stopped or reversed. Recovery is not guaranteed.
- Report suspected fraud at ReportFraud.ftc.gov. If your identity information was misused, use IdentityTheft.gov for a recovery plan.

Do not pay a stranger who promises to recover stolen money. Do not feel embarrassed about asking for help; act promptly.

Known help and official guidance

Bodell Bytes

Call or text (989) 492-0058

info@bodellbytes.com | www.bodellbytes.com

FTC consumer advice: consumer.ftc.gov

Fraud reports: ReportFraud.ftc.gov

Identity recovery guidance: IdentityTheft.gov

Source reading: FTC “How To Recognize and Avoid Phishing Scams”; “How To Spot, Avoid, and Report Tech Support Scams”; “Scammers use AI to enhance their family emergency schemes”; “Did a celebrity really endorse THAT? Maybe not”; and guidance on QR codes and verification codes. All are available at consumer.ftc.gov.

Our guide uses FTC guidance; FTC does not endorse Bodell Bytes. The visit is a check of agreed items at a point in time. It reduces risk and builds awareness; it cannot guarantee protection from every infection, scam or future threat.