Phelps Health
GOING BEYOND better

# STAYING SAFE ONLINE

## A Cybersafety and Identity Protection Guide

*For Phelps Health patients and our neighbors across south-central Missouri*

### In this guide, you'll learn how to:

- Practice everyday cybersafety
- Freeze and monitor your credit
- Report a cybercrime to the FBI

# WHY THIS MATTERS

Scammers increasingly target older adults, patients managing new diagnoses and rural communities where fewer people may have easy access to fraud-recovery help. Phelps Health created this guide so you and your family have a plain-language reference for protecting your personal information, finances and medical identity. Keep this packet somewhere handy or with other important papers.

# EVERYDAY CYBERSAFETY

## Passwords and Accounts

- Use a different password for each important account (email, banking, insurance portals). If one password leaks, the others stay safe.
- Make passwords long rather than clever—a phrase of four to five random words is stronger and easier to remember than a short jumble of symbols.
- Turn on multi-factor authentication (MFA) wherever it's offered. This sends a code to your phone or email so a stolen password alone won’t let scammers access the account.
- Consider a password manager (built into most phones and web browsers for free) so you don't have to memorize everything.

## Spotting Phishing and Scam Contact

- Be suspicious of unexpected calls, texts or emails that create urgency: “Your account will be closed,” “You owe money now” or “Your benefits are at risk.”
- Legitimate agencies (Social Security, Medicare, the IRS, Phelps Health billing) will not demand payment by gift card, wire transfer or cryptocurrency.
- Don't click links or open attachments from senders you don't recognize. Instead, go directly to the organization's website by typing the address yourself or calling the number on your billing statement or insurance card.
- Hang up and call back using a number you already know to be correct—never one given to you by the caller.
- Watch for health-specific scams: fake COVID/vaccine surveys, “free” medical equipment offers, fraudulent Medicare card replacement calls and phony insurance enrollment pitches.

## Devices and Home Network

- Keep your phone, computer and apps updated—updates often patch security holes.
- Use antivirus/security software on computers, and only download apps from official app stores.
- Set your home Wi-Fi router password to something unique, and avoid online banking or entering personal information over public Wi-Fi (library, coffee shop) unless you're using a trusted connection.
- Back up important documents and photos, either to an external drive or a reputable cloud service, in case of ransomware or device failure.

# LOCKING (FREEZING) AND MONITORING YOUR CREDIT

A credit freeze is one of the strongest, free protections available. It blocks lenders from viewing your credit file, which stops most new fraudulent accounts from being opened in your name. It does not affect your existing accounts or your credit score, and you can lift it whenever you apply for credit.

## Step 1: Freeze your credit at all three bureaus

You must contact each bureau separately—freezing one does not freeze the others. All three bureaus (listed below) are free and requests made online or by phone are applied within one business day.

Credit Bureau Contacts

- **Equifax:** *equifax.com/personal/credit-report-services/credit-freeze*, (888) 298-0045
- **Experian:** *experian.com/freeze*, (888) 397-3742
- **TransUnion:** *transunion.com/credit-freeze*, (800) 916-8800

Have this information ready when you call or apply online:

- Full name
- Date of birth
- Social Security number
- Current/previous addresses

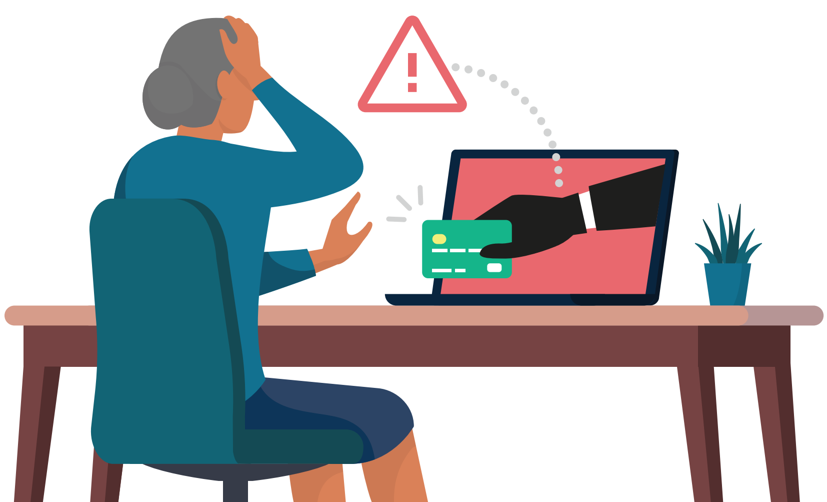
You'll receive a PIN or password. Save it somewhere safe—you'll need it to lift the freeze later.

## Step 2: Check your credit reports for free

- Visit *AnnualCreditReport.com* (the only federally authorized source) to get free reports from all three bureaus. Reports are available weekly at no cost.
- Review each report for accounts, addresses or inquiries you don't recognize.
- Be cautious of paid “credit monitoring” services. Monitoring your own free reports and keeping a freeze in place accomplishes the same goal at no cost.

## If you believe you're already a victim:

- Consider a fraud alert instead of, or alongside, a freeze. This requires lenders to verify your identity before opening new credit and is easier for family members to manage on your behalf.
- Visit *IdentityTheft.gov* (Federal Trade Commission) for a personalized, step-by-step recovery plan.
- Order copies of your medical records and an “Accounting of Disclosures” from Phelps Health or your insurer if you suspect medical identity theft (someone using your insurance information).



# REPORTING CYBERCRIME TO THE FBI

If you've been targeted by a scam, phishing attempt, ransomware or online fraud, reporting it helps investigators track patterns and can support recovery of stolen funds. Reporting quickly matters—the faster a fraudulent transfer is reported, the better the odds of stopping or reversing it.

## Where to report

FBI Internet Crime Complaint Center (IC3)

- **File a report online at *ic3.gov*:** This is the FBI's central hub for cyber-enabled crime and fraud reports.
- **Use IC3 for:** phishing, tech-support scams, romance/investment scams, ransomware, business email compromise and identity theft
- **If you or someone else is in immediate danger, call 911 or your local police first.**
- **To report an active threat or national security concern**, use *tips.fbi.gov* or contact your local FBI field office.

## What to have ready before you file

- Names, phone numbers, emails or websites used by the scammer
- Dates and a description of what happened
- Payment method used and where funds were sent (bank, wire, gift card, cryptocurrency wallet)
- Any screenshots, emails or texts you can save as evidence

## Also consider reporting to:

- Missouri Attorney General's Consumer Protection Hotline: (800) 392-8222
- Your local police department, especially if money or property was taken
- Your bank or credit card company **immediately** if a payment or account was involved

## MORE RESOURCES

- AARP Fraud Watch Network Helpline (free, open to all ages): (877) 908-3360
- *FTC IdentityTheft.gov*: personalized recovery plans for identity theft
- *AnnualCreditReport.com*: free weekly credit reports from all three bureaus
- Missouri Attorney General Consumer Protection: *ago.mo.gov* or (800) 392-8222
- FBI Internet Crime Complaint Center: *ic3.gov*
- Staying safe from MyChart scams and fraud: *mychart.org/l/en-us/help/staying-safe-from-scams-and-fraud*

*This guide is for general education and is not legal, medical or financial advice. Phone numbers and web addresses were verified as of July 2026 and may change—if a number no longer works, search the organization's official website directly.*