CITIZENS FRAUD UPDATE

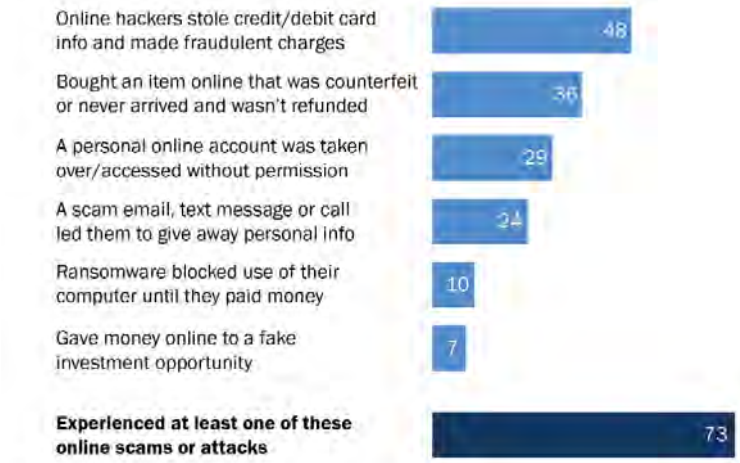
OCTOBER IS CYBERSECURITY AWARENESS MONTH

This month is a time dedicated to empowering individuals and organizations to protect themselves from digital threats. With fraud tactics growing more sophisticated every day—phishing scams, identity theft, data breaches—it's more important than ever to stay informed and alert. This month, we'll be sharing tips, tools, and insights to help you recognize fraud, safeguard your personal information, and build stronger cyber habits. Because staying secure online isn't just about technology—it's about awareness.

INSIDE THIS EDITION:

ROUGHLY THREE-QUARTERS OF AMERICANS HAVE EXPERIENCED AN ONLINE SCAM OR ATTACK

% of U.S. adults who say each of the following has happened to them



Note: "Bought an item online that was counterfeit or never arrived and wasn't refunded" was originally asked as two separate items; that figure includes those who say either or both has happened. Those who did not give an answer are not shown. Please refer to the questionnaire for full question wording.
Source: Survey of U.S. adults conducted April 14-20, 2025. "Online Scams and Attacks in America Today"

PEW RESEARCH CENTER

Citizens BANK MINNESOTA

WooHoo! Banking®

WooHoo! IT'S WHAT WE DO!

CHECK YOUR CYBERSECURITY SAFETY

Take this short quiz to find out how safe your cybersecurity habits are. Read the question and answer:
Always(3) Sometimes(2) Never(1)

1. **Do you keep your software up to date on your devices and computers?**
   - Tip – Updates are pushed out from companies as a way to patch security to any vulnerabilities that exist on their platforms. Delaying updates could leave you vulnerable to attacks.

2. **Do you have unique passwords for your online accounts?**
   - Tip- We know that trying to remember multiple passwords can be difficult, but did you know that reusing passwords is one of the easiest ways that hackers can gain access to multiple accounts if even one account is breached. Need help? Use a password manager to keep track of passwords that are strong and unique. See more information in the next article.

3. **Do you utilize two-factor authentication when it's available?**
   - Tip – Two-Factor Authentication (2FA) adds an extra level of security that goes above and beyond just using a password. Using app-based authenticators over receiving text message codes is even a higher level of security.

4. **Do you use public Wi-Fi cautiously?**
   - Tip – Public Wi-Fi is a favorite of hackers. You want to avoid public wi-fi especially when accessing personal data, like banking. Use a Virtual Private Network (VPN) or switch to mobile data when accessing sensitive accounts.

5. **Do you avoid clicking on ads or pop-ups from unknown sources?**
   - Tip- Clicking on ads or links from pop-ups or in app ads can lead to malware infections, phishing websites, or fraud. Use ad blockers and always be cautious of clicking on links.

6. **Do you verify website URLs before entering login or payment information?**
   - Tip- Be sure to verify that the domain includes https not just http. HTTP (HyperText Transfer Protocol) transfers data as plain text, making it insecure and vulnerable to interception, while HTTPS (HyperText Transfer Protocol Secure) uses encryption via SSL/TLS certificates to secure data transmission, preventing unauthorized access to sensitive information like passwords and credit/debit card numbers.

7. **Do you review app permissions and privacy settings on your phone and accounts?**
   - Tip- When you install an app or online service, it asks for permission to access parts of your device or personal information such as location, camera, microphone, contacts, browsing history, etc. How often do you click "allow" without a second thought? Be sure to read through and really dig into what an app might need.

8. **Do you know how to identify phishing emails or suspicious messages?**
   - Tip – Check the sender address carefully and watch for any minor changes. Use caution if there is any urgent or threatening remarks being used. Never click on unknown links or attachments. When in doubt, look up the official website on your own or call and ask questions using a verified number for that company.

9. **Do you back up your important data regularly?**
   - Backups protect you against ransomware, hardware failure, and accidental deletion. Use both cloud storage AND physical backups if possible.

10. **Do you securely dispose of old devices and hard drives?**
    - Tip – Simply deleting files isn't always enough. Make sure all data has been securely erased from a device before recycling or giving/selling your device to another user.

LET'S DIVE DEEPER – HERE'S A CLOSER LOOK AT SOME OF THE TOPICS FROM YOUR QUIZ

MANAGE APP PERMISSIONS FOR PRIVACY AND SECURITY

Apps often request access to sensitive data such as your **location, contacts, health info, camera, microphone**, and more. If not carefully managed, these permissions can expose your personal information to **data brokers, advertisers, or even malicious actors.**

THE PROBLEM:

- Many apps collect and sell data through permissions you grant—sometimes without clear disclosure.
- Sensitive data (like real-time location) can be used to build a detailed profile about you, including your daily habits and movements.

THE SOLUTION:

1. **Remove unused apps** – Unused apps still have access to your data unless deleted.
2. **Review app permissions** – Regularly check which apps have access to what data.
3. **Deny unnecessary access** – Only grant permissions essential for app functionality.
4. **Limit sensitive permissions like location tracking**—set it to "Only While Using App" where possible.
5. **Use official app store tools to** view what data an app collects before downloading.

BEST PRACTICES:

- Regularly audit your apps and their permissions.
- Revoke access to your camera, microphone, location, and other features unless required.
- Be extra cautious if you're at higher risk (e.g., activists, journalists, government personnel).
- **For device specific resources on how to manage app permissions please check:** IOS | Android | Mac | Windows

KEY TAKEAWAY:

You control your data. Don't give apps more access than they need—review, limit, and remove permissions regularly to protect your privacy and security.

YOUR SCORE:

25 – 30: CYBER GENIUS – Congratulations, you have excellent digital hygiene habits. Make sure to keep your guard up and stay in the know about proper digital habits.

15 – 25: ROOM TO IMPROVE – You're on the right track, but you can do a better job of protecting yourself, your family, and your employer. Focus on your weak points and be sure to implement some of the tips above.

0 – 15: HIGH RISK – It's time to get serious about cybersecurity. Please look over the tips above and implement these practices right away. Take some time to research the topics above. Get started TODAY!

BENEFITS OF USING A PASSWORD MANAGER

In today's digital world, we juggle dozens of online accounts—each needing a unique & secure password. But remembering them all? Nearly impossible. That's why password managers are essential tools for today's cyber world we live in.

What Is a Password Manager?

- Generates strong, random passwords for each account.
- Stores them securely in an encrypted vault, protected by a single master password.
- Fills in login info automatically on websites and apps.
- Flags weak, reused, or compromised passwords and suggests stronger alternatives.
- Helps you avoid phishing scams by warning you about fake sites.

Benefits of Using One:

- Stronger, unique passwords for every account.
- Less risk of identity theft or account takeovers.
- Time saved from typing or resetting forgotten passwords.
- Protection from reused passwords across different sites.

How to Choose the Right One. Look for features like:

- End-to-end encryption & zero-knowledge security.
- Compatibility across all your devices.
- Password audits and security alerts.
- Reasonable pricing (many offer free versions with basic features).

KEY TAKEAWAY:

Using a password manager is one of the simplest, most effective ways to protect yourself online and reduce your cybersecurity risks.

REAL LIFE SCAM

George sees an eye catching ad video on his phone: "Play quick games, win cash instantly — join now and cash out via PayPal!" The ad shows videos of people celebrating and 5 star ratings. George downloads the app by clicking the link displayed and creates an account. The app quickly gives a small test win — $2 — and prompts George to verify his phone number to cash out.

A few days later the app asks George to complete a "security check" to withdraw larger sums: upload a photo ID, link a PayPal or bank account, and pay a small "processing fee" to unlock withdrawals. The app also asks for permission to access contacts and location (so it can "find friends and nearby jackpots"). George grants the permissions to speed things along.

After paying the fee and uploading the ID, George's "balance" increases — but when he clicks Cash Out, the app shows a long "withdrawal processing" message. Customer support replies with canned responses and requests more fees for verification. When George finally stops paying and checks other app reviews, he finds hundreds of complaints describing the same pattern. The app is gone from the ad platform, the developer contact info is fake, and George now faces unauthorized charges on their card and a possible identity theft from someone abusing the uploaded ID.

SPOT THE RED FLAGS:

- The app was installed from a link or ad instead of the official app store.
- The app asks for a fee to withdraw winnings or "unlock" features.
- Requests for sensitive documents (government ID) or full bank account access.
- Permission requests that don't match the app's purpose (e.g., a simple game asks for SMS and contacts).
- Too good to be true promises ("$500/day playing for only 5 minutes").
- Poor grammar in app texts or support replies, or developer contact info that's generic.
- No verifiable company information, and many negative reviews describing nonpayment.

RESOURCES

For more information visit: citizensmn.bank/trending-security-topics. We add relevant topics about cybersecurity and spotlight ways to combat fraud!

Citizens Bank Minnesota:
507-354-3165 or
toll free at 800-549-0194

Identity theft questions? Contact your Social Security Office:
Mankato: 1-877-457-1734
Twin Cities: 1-800-772-1213
St. Cloud: 1-877-405-1446