ONLINE BANKING SECURITY 101:

How To Keep Your Money Safe

Bank Midwest

SECURITY IS OUR TOP PRIORITY:

We Care for Your Information Like It's Our Own

Each year, millions of consumers are impacted by fraud. In 2022, total losses exceeded $8 billion.[1]

The bad news? That figure is 30% higher than the previous year, with more fraud taking place via online and mobile channels, and less being reimbursed back to consumers.

The good news? There are more ways to protect yourself than ever before.

As an employee-owned community bank, our team at Bank Midwest is entirely aware of the enormous amount of trust our customers place in us to keep their money safe, which is why we spare no effort to protect their funds.

But today's fraudsters are circumventing security controls by manipulating users into giving away the keys to their fortunes. As such, being aware and proactive online has never been more important.

[1] https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

FIRST THINGS FIRST:

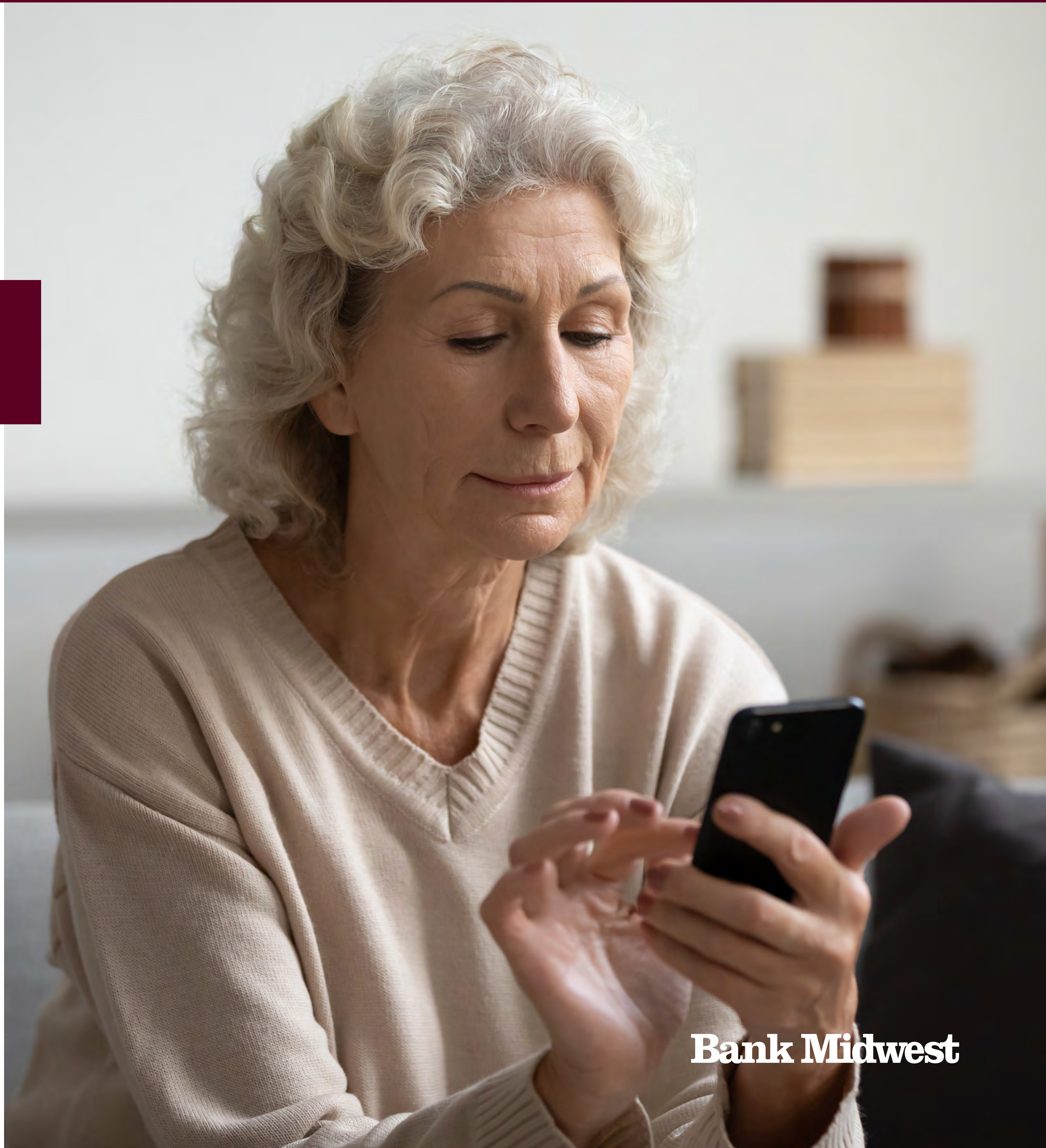
Know What To Look Out for

> "Pause. Trust your gut before you react. As the saying goes, 'If it sounds too good to be true, it always is!'"
>
> **–Stacie Wolter, Fraud Analyst**

The majority of cyberattacks start as phishing scams. Phishing refers to any attempt — online or over the phone — to manipulate users into downloading malware, giving away sensitive information or login credentials, or taking other actions that expose an individual to cybercrime, theft or fraud.

Be on the lookout for:

- **Emails and text messages** from unknown senders that contain mysterious links or file attachments.
- **Phone calls** from someone claiming to be from the IRS or any other agency claiming you owe money.
- **"Urgent" messages sent via email or text** that prompt you to share personal information (Social Security number, driver's license, name, address or date of birth, bank account information, etc.).
- **Anyone asking to confirm** your account details.
- **Time-sensitive password reset emails** that ask you to type in your old password.
- **Any message,** even from known contacts, that contains links or file attachments without any context.



When in Doubt, Reach Out

Let's say you receive an email or text message claiming one of your accounts has been compromised and you need to reset your password by clicking a link.

Or, you get a notification that your order has been received and your account will be debited a large amount of money. You need to call to cancel the order.

Do not take these messages at face value. Instead:

1. **Close the notification without clicking links, downloading attachments or calling any number listed in the email.**
2. **Delete the notification. Fraudsters are known to prey on emotions by inciting a sense of urgency. Never call a phone number listed in the notification received; always go to a trusted source.**

This will help you avoid falling prey to scammers who pose as real companies in an attempt to steal information that can be used for fraud.

Bank Midwest

Best Practices To Keep You Safe

In addition to vigilance and a healthy amount of skepticism, you can keep your information safe online and over the phone by taking the following actions:

Set Up or Update Your Privacy Code

As a Bank Midwest customer, you can set up a unique privacy code to help our team verify your identity. This privacy code makes it easier to determine whether it's really you who's connecting with us by phone or online. It also helps prevent fraudsters from reaching out on your behalf. Think of a piece of information that only you would know for this code and that is not easily found on social media or the internet. If you already have a privacy code set up but believe it may be easily guessed, request that we change it.

Patch Your Software

Up-to-date software often has the latest and best security measures in place. So, it's important to patch browser plugins, operating systems and mobile applications as soon as the new update becomes available. Also, turning on automatic updates can make this process a breeze.

Use a Strong, Unique Password

Hackers will stuff stolen credentials in as many online services as possible in the hope that those logins have been used elsewhere. Use a unique password for every website, preferably one that is 9-12 characters and contains numbers and symbols. Use a password manager if you need help remembering each one.

Additional Best Practices To Keep You Safe

Enable two-factor authentication

Two-factor authentication (2FA) lets you use a second factor (e.g., a phone call or text message) to verify login attempts on new devices. Set this up for social media accounts, email, online shopping and more to add an extra layer of protection to your profiles.

Avoid Sensitive Transactions on Public Wi-Fi

Public Wi-Fi is insecure, which means using it can make your device susceptible to hackers and viruses. It's best to avoid using public Wi-Fi for any tasks that involve sharing sensitive or personally identifiable information, including online banking and shopping.

Password Protect Your Devices and All Financial Apps

Use biometric authentication — like fingerprint and face scan — as well as for any finance apps that support it. This includes third-party apps that are connected to your bank account.

Go to your account settings in your apps to set up PINs or enable biometric login. This will help ensure that lost or unattended devices don't become vulnerable to fraud. Store money on non-bank financial apps sparingly: they may not be FDIC-insured.

Be Safe Offline

Promptly remove mail that arrives in your mailbox, avoid using unmarked ATMs, shield the keypad with your hand as you enter your PIN and shred physical documents with sensitive information.

How Bank Midwest Protects You

To help keep your accounts safe, the experts at Bank Midwest have implemented the following cybersecurity controls:

Chip Cards
Our EMV technology protects your debit card data during transactions.

SSL Encryption
We encrypt all of our web pages.

Account Lockout
Your account will lock access after multiple incorrect username or password entries.

Session Timeout
We automatically log you out of your online banking portal after 15 minutes of inactivity.

Real-Time Fraud Monitoring
Our team actively monitors accounts for suspicious activity and immediately notifies you if we spot anything amiss.

Alerts
We make it easy to set up alerts via mobile and online banking to help you maintain a close watch over account activity.

But even with these controls, it's critical that our customers understand the security risks of online use, and the actions they can take to minimize exposure.

IF YOU SUSPECT FOUL PLAY, CALL US RIGHT AWAY:

We’re Here To Help

> “Any time you question a suspicious transaction or urgent notification, don’t hesitate to reach out to Bank Midwest and ask if we can help determine whether it’s legitimate. In fact, it’s the best thing you can do.”
>
> **–Katie Siepker, Retail Operations Supervisor**

At Bank Midwest, we’ll gladly walk you through 10 false alarms if it means we never miss a real security incident. Contact us the second you suspect foul play. We’ll look into an incident for you and, should worse come to worst, guide you through remediation.

In the meantime, keep doing your part to secure your information on the web and we’ll keep doing ours to ensure that your funds stay under lock and key.

To learn more about how to stay safe on the web or to have your questions answered, contact our team or visit your local branch. We’re always glad to see you at Bank Midwest.

Contact us

Bank Midwest
BankMidwest.com ▪ Member FDIC