
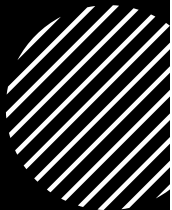



"Banking Made Easy: Online Banking"

Mankato Computer Technology University



Introduction: Why Online Banking?



Convenience, security, and control — no lines, no rush.



Stats on tech adoption (e.g., “78% of people over 50 now own a smartphone”).



Global Usage



Over **2.5 billion people worldwide** used **online or mobile banking** in 2024.



This number is expected to grow to **3.6 billion by 2027**, driven by smartphones and digital banking services.

us United States

- About **78% of U.S. adults** used **online banking** in 2024.
- Around **66%** used **mobile banking apps** specifically.
- **Baby Boomers (ages 60–78):**
 - Over **60%** use online banking regularly
 - About **40%** use mobile apps — a number that continues to grow each year
- “Nearly 4 in 5 Americans bank online.”
- “More than half of Baby Boomers now log in from home instead of visiting a branch.”
- “Digital banking adoption among Boomers rose by 25% in the past 5 years.”

What Is Online Banking?

- **Online banking** allows people to manage their bank accounts over the internet — anytime, anywhere — without visiting a physical bank branch.




Benefits of Online Banking

- **24/7 Access:** Check your balance, pay bills, or transfer money anytime.
- **Convenience:** Avoid lines and save trips to the bank.
- **Speed:** Transactions are processed quickly.
- **Paperless:** View statements and bills electronically.
- **Security:** Banks use encryption and multi-factor authentication (MFA) to protect accounts.





What You Can Do With Online Banking

- **Check Account Balances & Transactions**
 - **Transfer Money**
 - Between your accounts
 - To others (e.g., Zelle, Interac e-Transfer)
 - **Pay Bills Online**
 - Schedule one-time or recurring payments
 - **Deposit Checks Remotely**
 - Use your smartphone camera via your bank's app
 - **View E-Statements**
 - Digital versions of monthly bank statements
 - **Apply for Loans or Credit Cards**
 - Submit applications online
- 



Is Online Banking Safe?

- Yes — with proper precautions:
 - **Use strong, unique passwords**
 - **Enable two-factor authentication (2FA)**
 - **Watch for phishing emails or fake websites**
 - **Avoid using public Wi-Fi for banking**
 - Most banks use:
 - End-to-end encryption
 - Fraud detection systems
 - 24/7 account monitoring
- 
- 



What Is 2FA?

- It means you need **two things** to log in:
- **Something you know**
→ Your **password**
- **Something you have**
→ A **code sent to your phone**, a **security app**, or even a **fingerprint**

Example

- You log in to your bank account using your password.
Then, your bank sends a **6-digit code to your phone**.
You must enter that code to access your account.
- Even if a scammer gets your password, they **can't log in** without that second code.



Common 2FA Methods:



Text message (SMS)
code 📱



Authenticator app (e.g.,
Google Authenticator,
Authy) 🔑



Biometric (Face ID or
fingerprint) 🖐️



Email confirmation ✉️

Why It Matters for Banking



Prevents
unauthorized
access



Protects your
money



Makes you **much
harder to hack**

How to Get Started

1

Visit your bank's website or download their mobile app

2

Register using your account number and personal info

3

Create a username & password

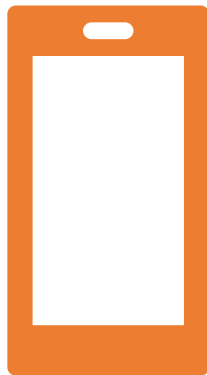
4

Set up security questions & 2FA

5

Log in & explore features

Getting Started: What You'll Need



Device (computer/tablet/smartphone),
internet, and a bank account.



Setting up strong passwords & 2FA
explained simply.

Common Features You'll Use



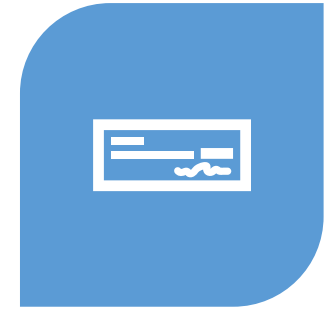
CHECKING BALANCES



PAYING BILLS



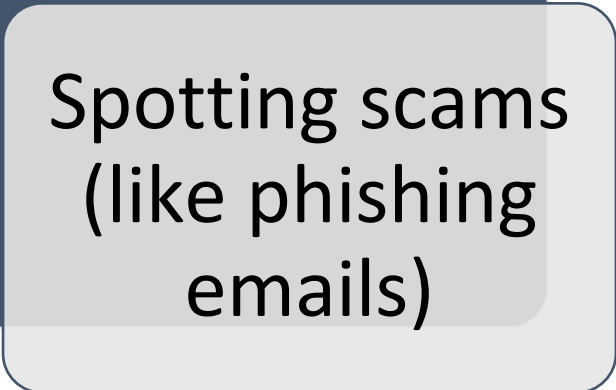
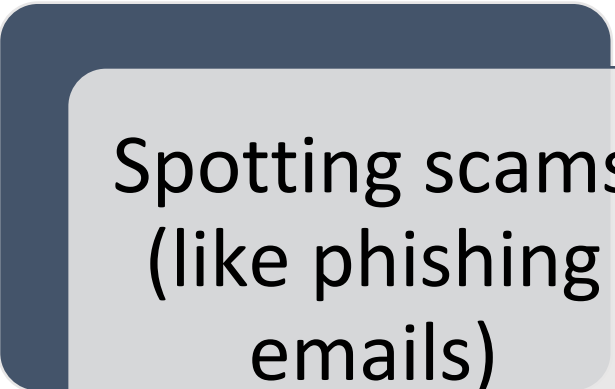
TRANSFERRING MONEY



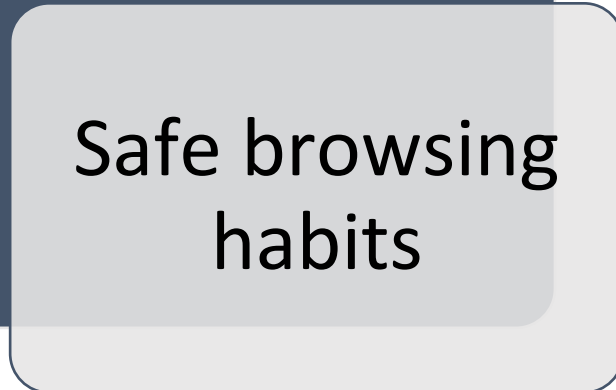
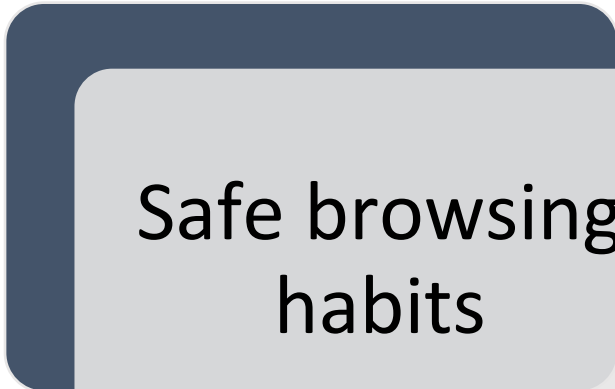
DEPOSITING CHECKS WITH
YOUR PHONE



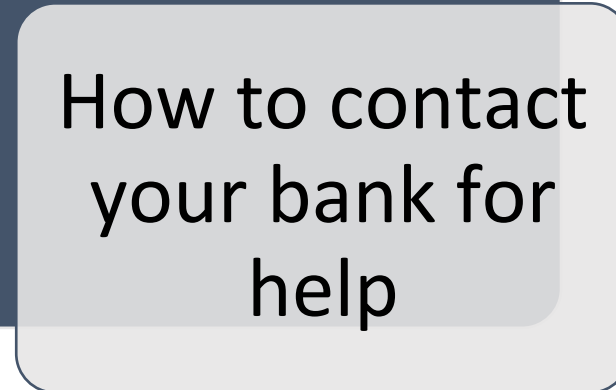
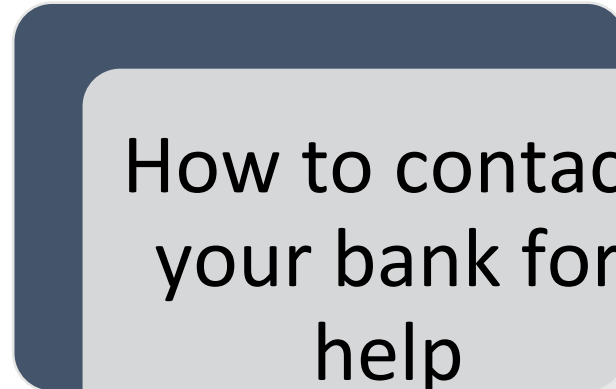
Staying Safe Online



Spotting scams
(like phishing
emails)



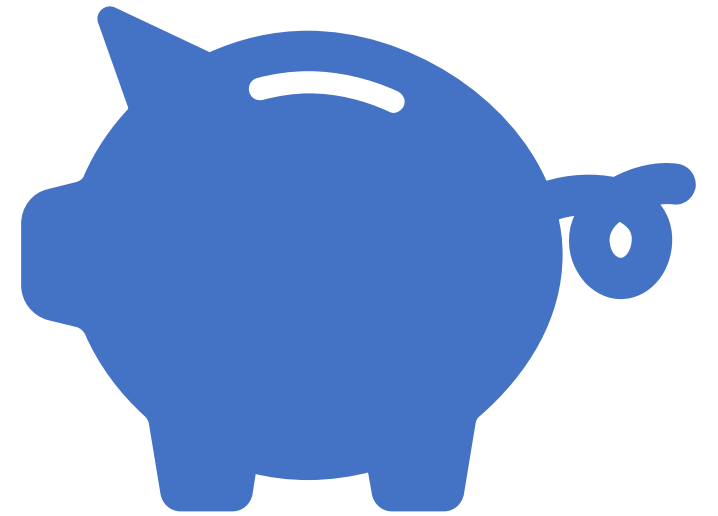
Safe browsing
habits



How to contact
your bank for
help

Online Banking Scams: What You Need to Know

- Scammers try to trick you into giving them access to your bank account. But don't worry — knowing the signs can help you stay safe.





Common Online Banking Scams



Phishing Emails & Texts



“Your account is locked — click here to verify!”



Looks like it's from your bank, but it's fake.



Clicking the link may steal your login info.



Stay Safe:

Don't click links in unexpected emails or texts. Always go directly to your bank's website.

Fake Bank Websites



Look identical to your real bank site, but are set up to steal your info.



Stay Safe:

Check the web address — it should start with <https://> and use your bank's exact domain (like wellsfargo.com or chase.com).

Tech Support Scams

“I’m calling from Microsoft — your account has been hacked.”

The scammer may ask to remotely access your device.



Stay Safe:

Banks and real tech companies never call you out of the blue to fix something.

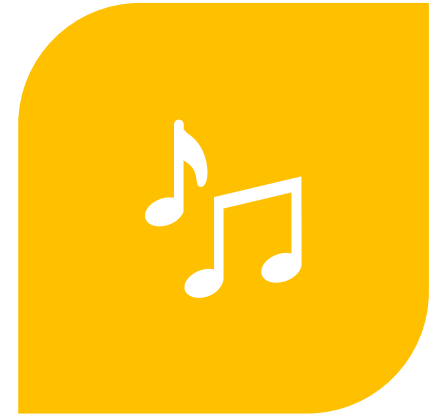
“Too Good to Be True” Offers



“GET \$500 FOR TAKING A SURVEY!”



OFTEN LEADS TO MALWARE OR ASKS
FOR YOUR BANKING INFO.



 **STAY SAFE:**
IF IT SOUNDS TOO GOOD TO BE TRUE,
IT PROBABLY IS.

Fake Bank Representatives

You get a call or text from someone pretending to be from your bank.



Stay Safe:

Hang up and call your bank directly using the number on your debit card.

How to Protect Yourself

- ☒ Use **strong, unique passwords**
- ☒ Turn on **two-factor authentication (2FA)**
- ☒ Keep your **banking app and device software up to date**
- ☒ Never share your login info — not even with family
- ☒ **Log out** when done, especially on shared devices