Online Banking Safety

Passwords & Protection

Why it Matters:

Your online banking account holds your most sensitive financial information. Strong passwords and smart habits are your first line of defense against fraud and identity theft.

What Makes a Strong Password?

A strong password is:

- At least 12 characters
- A combination of upper and lower-case letters, numbers and special characters
- Does not use personal information
- A unique password for every account
- Not a common word or phrase (avoid “password123” or your name)

Top Online Banking Safety Tips:

- Use Multi-factor Authentication (MFA): Always enable 2-step verification (like a text code or authentication app)
- Change Passwords regularly: Update your passwords every 3-6 months
- Never Share Passwords: Not with friends, not over text, not in emails
- Avoid Public Wi-Fi for Banking: Use secure, private connections or a VPN when accessing your banking
- Log Out After Each Session: especially on shared or public devices
- Watch for Phishing Scams: Don’t click suspicious links or open unexpected emails/texts from your bank
- Monitor your Account Often: Set up alerts and check transactions weekly
- Use a Password Manager: it’s tough to remember a lot of strong passwords. Use a secure password manager to store and generate them safely.
- Use a Passphrase: A long sentence can be easier to remember and still secure. Example: MyDogEats@7AM&LovesToRun!

EXPERIENCE COMMUNITY

UNITY BANK

www.unitybanking.com