

# CYBERSECURITY TIPS

These best practices may help safeguard your identity and financial information.

## Protect Your Accounts

- Use strong, unique passwords for each account.
- Enable multi-factor authentication (MFA) whenever possible.
- Change passwords regularly—especially for sensitive accounts like banking, email, and insurance.

## Keep Your Devices Secure

- Install and regularly update antivirus and security software.
- Keep operating systems, browsers, and apps up to date.
- Avoid using public Wi-Fi for sensitive transactions unless connected to a secure VPN.

### Resources:

[FTC Online Security](#)

[CISA Tips](#)

## Monitor for Suspicious Activity

- Review bank and credit card statements monthly.
- Check your credit reports regularly (AnnualCreditReport.com offers free reports).
- Consider setting fraud alerts or a credit freeze with credit bureaus if suspicious activity is detected.

## Watch Out for Scams & Phishing

- Do not click suspicious links in emails or text messages.
- Be cautious of unsolicited calls or emails asking for personal or financial information.
- Legitimate companies will never request passwords or Social Security numbers through email or over the phone.

## Practice Safe Online Habits

- Limit the personal information you share online.
- Be careful with what you post on social media, as it can be used in identity theft schemes.
- Regularly back up important data to a secure location.



**Diversified LLC**  
**diversifiedllc.com**

