Software Update Guide

Software Update Guide

Windows Computers

1. **Open Settings**
2. Click on the Start button (Windows icon) in the bottom-left corner
3. Click on the gear icon (Settings)
4. **Navigate to Update & Security**
5. In the Settings window, scroll down and click on "Update & Security"
6. **Check for Updates**
7. In the left panel, make sure "Windows Update" is selected
8. Click the "Check for updates" button
9. Wait for the scan to complete
10. **Install Available Updates**
11. If updates are found, click "Download and install"
12. Follow any on-screen prompts
13. Save your work before installing updates that require a restart
14. **Restart Your Computer**
15. When prompted, click "Restart now" to complete the installation
16. If you need to finish work first, select "Schedule the restart" instead

iPhone/iPad Devices

1. **Open Settings**
2. Tap the Settings app (gray gear icon)
3. **Navigate to General**
4. Scroll down and tap "General"
5. **Check for Software Update**

6. Tap "Software Update"
7. Wait for the device to check for updates
8. **Install Available Updates**
9. If an update is available, tap "Download and Install"
10. Enter your passcode if prompted
11. Agree to the terms and conditions
12. **Important Notes**
13. Connect to Wi-Fi before updating
14. Make sure your device has at least 50% battery or is plugged in
15. Updates may take 15-30 minutes to complete

Android Devices

1. **Open Settings**
2. Tap the Settings app (gear icon)
3. **Navigate to System Updates**
4. Scroll down to "System" or "About Phone"
5. Tap "System Updates" or "Software Updates"
6. (Note: Menu names may vary by device manufacturer)
7. **Check for Updates**
8. Tap "Check for updates"
9. Wait for the device to check for available updates
10. **Install Available Updates**
11. If an update is available, tap "Download" or "Install"
12. Follow any on-screen prompts
13. Enter your PIN or pattern if prompted
14. **Important Notes**
15. Connect to Wi-Fi before updating
16. Make sure your device has at least 50% battery or is plugged in
17. Updates may take 15-30 minutes to complete

Making Updates a Habit

1. **Set a Monthly "Update Day"**
2. Choose a specific day each month (e.g., first Sunday)
3. Mark it on your calendar
4. My Update Day: _____
5. **Create Reminders**
6. Set a recurring reminder on your phone or calendar
7. Place a note on your refrigerator or bulletin board
8. **Update All Devices**
9. Update all your devices on the same day:
    - Computer
    - Phone
    - Tablet
    - Other smart devices
10. **Troubleshooting Common Issues**
11. Not enough storage space: Delete unused apps or photos
12. Slow internet: Schedule updates overnight
13. Update fails: Restart device and try again
14. Need help? Contact local resources listed on the Resources handout

---

Passphrase Creation Worksheet

Passphrase Creation Worksheet

The Story Method for Creating Strong Passphrases

What Makes a Strong Passphrase?

- **Length**: At least 16 characters (longer is stronger)
- **Complexity**: Mix of uppercase, lowercase, numbers, and symbols
- **Memorability**: Based on personal stories or memories
- **Uniqueness**: Different for each important account

Step 1: Choose a Personal Memory

Think of a specific memory, event, or object that is meaningful to you but not widely known: - First car you owned - Memorable vacation - Childhood home - Special gift you received - Favorite meal or recipe

My memory (write brief notes only): _____

Step 2: Include Specific Details

Add specific details that only you would remember: - Year it happened - Colors involved - Names of people or places - Amounts or measurements - Unique characteristics

Important details: _____

Step 3: Transform into a Passphrase

Convert your memory into a passphrase by: - Combining the key elements - Removing spaces - Adding capital letters - Including numbers - Adding symbols (!, @, #, $, %, etc.)

Example Transformation: - Memory: "I bought my first car in 1975, a blue Ford that cost $750" - Passphrase: "1stCar1975BlueFord!$750"

Step 4: Test Your Passphrase

A strong passphrase should: - Be easy for you to remember - Be difficult for others to guess - Include at least 16 characters - Contain uppercase and lowercase letters - Include numbers and symbols

Passphrase strength checklist: - [ ] At least 16 characters long - [ ] Contains uppercase letters - [ ] Contains lowercase letters - [ ] Contains numbers - [ ] Contains symbols - [ ] Based on personal memory - [ ] Not used for any other account

Step 5: Create Account-Specific Variations

For different accounts, modify your base passphrase: - Add the service name: "1stCar1975BlueFord!$750_Email" - Change specific elements: "1stCar1975BlueFord!$750" → "1stHouse1982Green!$120K" - Develop a pattern only you know

Remember:

- Never share your passphrase with anyone
- Don't write it down where others can find it
- Consider using a password manager to store your passphrases
- Change passphrases if you suspect they've been compromised

Note: This worksheet is for practice only. Do not write down your actual passphrases.

Password Manager Comparison Sheet

Password Manager Comparison Sheet

What is a Password Manager?

A password manager is a secure digital vault that stores all your passwords in an encrypted format. You only need to remember one master password to access all your other passwords.

Benefits of Using a Password Manager

- **Security**: Store unique, strong passwords for each account
- **Convenience**: Auto-fill login forms on websites and apps
- **Organization**: Keep track of all your accounts in one place
- **Generation**: Create strong passwords automatically
- **Cross-Device**: Access your passwords on all your devices

Popular Password Manager Options

Free Options

Bitwarden

- **Best for**: Beginners looking for a simple, secure solution
- **Platforms**: Windows, Mac, iOS, Android, all major browsers
- **Key Features**:
- Unlimited passwords on unlimited devices
- Basic password generation
- Secure notes storage
- Self-hosting option for advanced users
- **Limitations**: Some advanced features require premium version
- **Ease of Use**: ★★★★☆ (Very easy)

LastPass Free

- **Best for**: Users who primarily use one device type
- **Platforms**: Windows, Mac, iOS, Android, all major browsers

- **Key Features**:
- Unlimited passwords on unlimited devices of same type
- Password generator
- Secure notes
- Security challenge (password strength analysis)
- **Limitations**: Free version limits use to either mobile or computer devices
- **Ease of Use**: ★★★★☆ (Very easy)

Google Password Manager

- **Best for**: Google/Chrome users
- **Platforms**: Chrome browser, Android devices
- **Key Features**:
- Seamless integration with Chrome and Android
- Password generation
- Password checkup (breach alerts)
- **Limitations**: Limited to Google ecosystem
- **Ease of Use**: ★★★★★ (Extremely easy)

Apple Keychain

- **Best for**: Apple device users
- **Platforms**: Safari browser, iOS, macOS
- **Key Features**:
- Seamless integration with Apple devices
- Password generation
- Two-factor authentication code generation
- **Limitations**: Only works within Apple ecosystem
- **Ease of Use**: ★★★★★ (Extremely easy)

Paid Options

1Password

- **Cost**: $2.99/month (individual), $4.99/month (family)
- **Best for**: Families and Apple users
- **Key Features**:
- Family sharing (up to 5 users)
- Travel mode for border crossings

- Watchtower (security monitoring)
- Local storage option
- **Ease of Use**: ★★★★☆ (Very easy)

Dashlane

- **Cost**: $4.99/month (individual), $7.49/month (family)
- **Best for**: Users wanting extra security features
- **Key Features**:
- Includes VPN service
- Dark web monitoring
- Automatic password changing
- Digital legacy feature
- **Ease of Use**: ★★★★☆ (Very easy)

Getting Started with a Password Manager

Basic Setup Steps (for most password managers)

1. Create an account and set a strong master password
2. Install browser extensions and mobile apps
3. Begin saving passwords as you log into websites
4. Import existing passwords (if available)
5. Set up emergency access for trusted contacts

Tips for Success

- Start with just a few important accounts
- Use the password generator for new accounts
- Set up two-factor authentication for your password manager
- Write down your master password and store it securely
- Consider sharing access with a trusted family member

Emergency Access Planning

Most password managers offer ways for trusted contacts to access your vault in an emergency:

- **Designated Emergency Contacts**: Specify who can request access
- **Waiting Period**: Set a time delay (e.g., 48 hours) before access is granted

- **Approval Process**: You'll be notified and can deny access if it's not a true emergency
- **Legacy Planning**: Include password manager information in your estate planning

Recommended Option for Beginners

Bitwarden offers the best balance of security, ease of use, and features for most beginners, with a free tier that includes all essential features.

Multi-Factor Authentication Setup Instructions

Multi-Factor Authentication (MFA) Setup Instructions

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) adds an extra layer of security to your accounts by requiring two or more verification methods: 1. Something you know (password) 2. Something you have (phone or security key) 3. Something you are (fingerprint or face)

Why Use MFA?

- Protects your account even if your password is compromised
- Prevents unauthorized access from hackers
- Alerts you to potential break-in attempts
- Required by many financial institutions and email providers

Setting Up MFA on Common Services

Gmail / Google Account

1. Sign in to your Google Account at accounts.google.com
2. In the navigation panel, click **Security**
3. Under "Signing in to Google," click **2-Step Verification**
4. Click **Get started**
5. Follow the on-screen steps to set up text message verification

6. Enter the verification code sent to your phone
7. Click **Turn on** to enable 2-Step Verification

Yahoo Mail

1. Sign in to your Yahoo account
2. Click on your name or profile icon in the upper right corner
3. Select **Account info**
4. Click **Account security** in the left sidebar
5. Click **Two-step verification** and toggle it **On**
6. Enter your phone number and click **Send code**
7. Enter the verification code sent to your phone
8. Click **Verify** to complete setup

Microsoft Account (Outlook, Hotmail)

1. Sign in to your Microsoft account at account.microsoft.com
2. Select **Security** from the top navigation bar
3. Select **Advanced security options**
4. Under "Two-step verification," select **Turn on**
5. Follow the on-screen instructions to set up your verification method
6. Enter the code sent to your phone
7. Click **Next** and then **Finish** to complete setup

Facebook

1. Sign in to your Facebook account
2. Click the down arrow in the top right corner
3. Select **Settings & Privacy**, then **Settings**
4. Click **Security and Login** in the left sidebar
5. Scroll to "Two-Factor Authentication" and click **Edit**
6. Select **Text Message (SMS)** as your security method
7. Enter your phone number and click **Continue**
8. Enter the code sent to your phone
9. Click **Continue** to complete setup

Setting Up Backup Methods

Recovery Codes

1. During MFA setup, most services offer recovery codes

2. Write these codes down on paper and store in a secure location
3. Keep a copy with your important documents
4. Never store recovery codes digitally without encryption

Backup Phone Number

1. Add a trusted family member's phone number as a backup
2. During MFA setup, look for "Add backup method" or similar option
3. Select "Add phone number" and enter the backup number
4. Verify the number by entering the code sent to that phone

Backup Email

1. Add a secondary email address to your account
2. Look for "Recovery email" or "Alternate email" in account settings
3. Enter a different email address that you can access
4. Verify by clicking the link sent to that email address

Troubleshooting MFA Issues

Lost Phone

1. Use your recovery codes to sign in
2. If you don't have recovery codes, use your backup phone number
3. As a last resort, contact the service's customer support

New Phone

1. Sign in using your old phone before switching
2. Update your MFA settings with your new phone number
3. If you've already switched phones, use recovery codes to sign in

No Cell Phone

If you don't have a cell phone, alternative options include: 1. Email verification (where available) 2. Authentication apps on tablets or iPods 3. Printed backup codes 4. Security keys (physical USB devices)

Remember

- Always set up backup methods when enabling MFA
- Print and securely store recovery codes
- Update your MFA settings when you change phone numbers

- Test your recovery methods before you need them

Security Action Plan Checklist

Security Action Plan Checklist

Your Personal Digital Security Plan

Software Updates

- [ ] Set my monthly "Update Day": _____ (e.g., first Sunday of each month)
- [ ] Create calendar reminder for Update Day
- [ ] Update Windows computer
- [ ] Update iPhone/iPad
- [ ] Update Android device
- [ ] Update other smart devices (list): _____

Strong Passphrases

- [ ] Create strong passphrases for these critical accounts:
- [ ] Primary email account
- [ ] Banking/financial accounts
- [ ] Social media accounts
- [ ] Shopping accounts with payment information
- [ ] Other important accounts: _____
- [ ] Use the Story Method to create memorable but secure passphrases
- [ ] Ensure each passphrase is at least 16 characters long
- [ ] Include uppercase letters, lowercase letters, numbers, and symbols
- [ ] Use unique passphrases for each important account

Password Manager

- [ ] Select a password manager: _____ (recommendation: Bitwarden)
- [ ] Set up password manager account with strong master password
- [ ] Install password manager on:
- [ ] Computer browser
- [ ] Smartphone
- [ ] Tablet

- [ ] Save passwords for at least these accounts:
- [ ] Email
- [ ] Banking
- [ ] Social media
- [ ] Shopping
- [ ] Set up emergency access for trusted contact: _____

Multi-Factor Authentication (MFA)

- [ ] Enable MFA on these accounts:
- [ ] Primary email account
- [ ] Banking/financial accounts
- [ ] Social media accounts
- [ ] Shopping accounts with payment information
- [ ] Cloud storage (Google Drive, Dropbox, etc.)
- [ ] Set up backup methods:
- [ ] Print and store recovery codes in secure location: _____
- [ ] Add trusted backup phone number: _____
- [ ] Add recovery email address: _____

Implementation Timeline

Week 1: - [ ] Update all devices - [ ] Set up password manager - [ ] Create strong passphrase for email account

Week 2: - [ ] Enable MFA on email account - [ ] Create strong passphrases for financial accounts - [ ] Add financial accounts to password manager

Week 3: - [ ] Enable MFA on financial accounts - [ ] Create strong passphrases for social media accounts - [ ] Add social media accounts to password manager

Week 4: - [ ] Enable MFA on social media accounts - [ ] Create strong passphrases for shopping accounts - [ ] Add shopping accounts to password manager

Local Help Resources

- Senior Center Tech Support: Tuesdays 1-3pm
- Library Computer Assistance: By appointment
- Community College Free Workshops: Monthly
- Volunteer Tech Help Program: Call 555-123-4567

Notes

Remember: Start small and build gradually. Even implementing just one security measure is better than none!

Security Awareness Resource | © 2025 Security Awareness Initiative