FightCybercrime.org

#SecureTogether

STEP 1
TURN ON MULTIFACTOR AUTHENTICATION (MFA) FOR YOUR EMAIL

What is multifactor authentication?

Your online accounts are protected by passwords, but you can add more protection by using multi-factor authentication, sometimes called two-factor authentication (2FA).

Multi-factor authentication adds an extra layer of security to your accounts so that even if someone knows your password, they won't be able to log in without the additional verification.

It requires you to provide an additional verification factor, such as a notification sent through your mobile device, to log into an account or application.

Accounts implement MFA in a variety of ways. Receiving codes via text message or email is the only option for some online services. However, it is even safer to set up MFA using an authentication app.

Why is this important?

Criminals buy and sell information stolen in data breaches, including passwords. In addition, some may use software that can crack weak or reused passwords. That means that a password alone might not be enough to protect you. In addition to using a strong, unique password, multi-factor authentication provides an added layer of security to help prevent these types of breaches.

Go to the next page to learn how to set up MFA.

How do I set up multi-factor authentication for my email account?

Some email providers work with authentication apps like Authy or Google Authenticator. Others only allow you to set up MFA via email or SMS (text message).

- [ ] **Follow the instructions for one of the following popular email providers below.**

  AOL: help.aol.com/articles/2-step-verification-stronger-than-your-password-alone

  Gmail: www.google.com/landing/2step/

  Outlook: www.support.microsoft.com/en-us/account-billing/turning-two-step-verification-on-or-off-for-your-microsoft-account-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca

  Yahoo! Mail: www.yahoo-helpline.com/blog/yahoo-mail-two-factor-authentication-how-and-why-to-use-it/

- [ ] **If you want to set up MFA on your other accounts, visit 2fa.directory and follow the instructions for each site you use.**

  For more security, we recommend setting up MFA on bank accounts and social media profiles as well.

STEP 2
TIGHTEN YOUR ACCOUNT PRIVACY SETTINGS

What are privacy settings?

Many products, apps, and services allow you to control some aspects of how your personal information is collected, used, shared, or displayed.

#SecureTogether

Why is this important?

While it's impossible to control data collection entirely, some privacy settings might restrict the way companies can use, share or retain your location data, audio and video recordings, or other personal information. They can also give you some control over whether your social media posts are displayed publicly, and who they're displayed to.

How to tighten your privacy settings:

- [ ] **Decide which accounts to start with.**

  Most products, apps, and services provide some settings for controlling aspects of how your personal data is collected, used, and shared. Your email and social media accounts are probably the most important places to start.

- [ ] **Follow the instructions for one of the following popular online platforms with privacy settings below.**

  Apple: https://www.apple.com/privacy/manage-your-privacy/

  Facebook: https://www.facebook.com/help/443357099140264

  Google: https://safety.google/privacy/privacy-controls/

  Instagram: https://help.instagram.com/196883487377501

  LinkedIn: https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview?lang=en

  Microsoft: https://account.microsoft.com/account/privacy

  Snapchat: https://support.snapchat.com/en-US/a/privacy-settings

  TikTok: https://support.tiktok.com/en/privacy-safety/comment-duet-and-direct-message-control-default

  Twitter: https://help.twitter.com/en/safety-and-security#ads-and-data-privacy

  Verizon: https://www.verizon.com/privacy/your-data

Completed this step?
Go to the next page.

#SecureTogether

STEP 3
STAY UPDATED ON YOUR ACCOUNTS

Update Your iPhone, iPad, or iPod Touch

Upgrade to the latest version of iOS or iPadOS for security updates and bug fixes, as well as new features.

Why is this important?

Each new iOS or iPadOS software update includes bug fixes that protect your phone or tablet from known security risks.

How do I update my device?

- ☐ Find the update in Settings > General > Software Update. If one is available, tap "download and install."
- ☐ If you see a message asking you to temporarily remove apps to make space for the update, click "continue." The apps will be automatically reinstalled after the update.
- ☐ Set up automatic updates so you'll always have the latest protections against malware and vulnerabilities. Go to Settings > General > Software Update, and select "Automatic updates."

Troubleshooting:

There may be times when you'll need to make space for an update by manually deleting content from your device.

If you don't want to do so, you can update by connecting your device to a Mac laptop or desktop computer. Make sure the computer is connected to a WiFi or Ethernet network, rather than the personal hotspot on the device you're updating.

Locate the device using "Finder" and "Location" on Catalina (or iTunes on macOS Mojave), then clicking "General" and clicking "Check for Update." Click "Download and Update," and enter your passcode if prompted.

#SecureTogether

Update Your Android Phone

Update to the latest version of Android for security updates and bug fixes, as well as new features.

Why is this important?

Each new Android software release and security update includes bug fixes that protect your phone from known security risks.

How do I update my device?

- ☐ Open your Settings app by tapping Settings > System > Advanced > System Update to see your update status. If an update is available, follow the steps on the screen.
- ☐ Google will release updates for security reasons and to introduce new features. These should download automatically, but you may want to check for updates on your own if your device has been offline. Go to Settings > Security > Security Updates. Follow the instructions on the screen.
- ☐ Update the apps on your phone, too. Go to Settings > Security > Google Play system update to see if any updates through the Google Play system are available.
- ☐ Set your apps to update automatically by going to Google Play Store > Profile > Settings > Network Preferences > Auto update apps. You can set them to update on any network using WiFi or mobile data, or to update only when connected to WiFi.

Troubleshooting:

There may be times when you'll need to make space for an update by manually deleting content from your device. Android support has tips and directions on how to do that.

If an update starts downloading but doesn't finish, your device will send you a notification when it automatically tries to download again. Open the notification and tap the update action.

Update Your Mac Operating System

Keeping your operating system up to date is one of the simplest and most important steps you can take to protect yourself from software vulnerabilities.

Why is this important?

Many kinds of viruses and malware work by taking advantage of security vulnerabilities in software that is out of date.

How do I update my Mac?

- ☐ Update your software. Go to Apple menu > System Preferences > Software Update. If an update is available, click "Update now."
- ☐ To automatically install macOS updates, select "Automatically keep my Mac up to date." Click "OK."
- ☐ To receive all of the latest updates automatically, click on Advanced and select "Check for updates," "Download new updates when available," "Install MacOS updates," "install app updates from the App Store" and "Install system data files and security updates."

Update Your Windows Operating System

Keeping your operating system up to date is one of the simplest and most important steps you can take to protect yourself from software vulnerabilities.

Why is this important?

Many kinds of viruses and malware work by taking advantage of security vulnerabilities in software that is out of date.

How do I update my Windows PC?

- ☐ Windows should automatically download and install important security updates for your PC. To check for software updates manually, select Start > Settings > Update & Security > Windows Update. Select "check for updates." If an update is available, follow the instructions on the screen.
- ☐ Windows can automatically update your apps, too. Click on the Start Screen, then select "Microsoft store." Select the account menu (the three dots) and click on Settings > App updates. Set "Update apps automatically" to "On."

STEP 4
PROTECT YOURSELF FROM PHISHING

Phishing occurs when an attacker sends a fake message designed to trick you into providing private information, like a password, or downloading harmful software like ransomware or a virus. They may try to steal your username and passwords, or even your identity and financial assets.

Why is this important?

Phishing attempts can be effective because they are often designed to look like they come from someone you know or a website or company you trust. While these attempts can be hard to spot, many of them can be prevented if you're aware of them or know what to look for.

There are many different types of phishing, which can happen over email, text message, messaging apps or even phone or voicemail. In real life, phishing attempts are harder to stop because they've become more sophisticated over the years.It is common to get caught because they've been designed to provoke participation. Below is a fictitious, dramatic example we made up. See how many red flags you can spot! (Answer key on next page.)

Scenario:

Sara received an urgent email from her bank account asking for immediate action. Sara isn't sure what to do and needs your help. Read the email below and try to spot anything that looks suspicious.

From: Trusted Bank <trustedbank@hotmail.com>
To: Sara Jorge <sarajorge@gmail.com>
Subject: Immediate Action Required: Update Bank Information

Dear Valued Customer,

It has come to our attention that there has been a billing error associated with your account. Due to the error, we have suspended your account until reviewing the issue and proper verfication has occured.

To access and reactive your account, simply click the link below and follow the steps to enter your account details and password.

www.trustedbank.eg/activation

If completed within the next 48 hours, your account will resume as normal.

Thank you,
Trust Bank Custumer Service Team
For customer service inquires call 1-866-397-8541

#SecureTogether

Answer Key:

From: Trusted Bank <trustedbank@hotmail.com> **1** Hotmail Address
To: Sara Jorge <sarajorge@gmail.com>
Subject: Immediate Action Required: Update Bank Information **2** Requiring immediate or urgent action

Dear Valued Customer,

It has come to our attention that there has been a billing error associated with your account. Due to the error, we have suspended your account until reviewing the issue and proper verfication has occured. **3** Says your account is on hold
To access and reactive your account, simply click the link below and follow the steps to enter your account details and password. **4** Ask you to update your information by reentring your personal information and password

www.trustedbank.eg/activation **5** Uses an unfamiliar domain (in this case ".eg")

If completed within the next 48 hours, your account will resume as normal.

Thank you, **6** Spelling error
Trust Bank Custumer Service Team
For customer service inquires call 1-866-397-8541

Here's what to do to spot malicious sites or phishing attempts

1. Verify! When you receive a new message—especially one that looks suspicious, urgent, or unexpected—look closely at the email address, phone number, or social account it came from. Do you recognize it? Be suspicious of an email, text, social media message or even phone call asking you to reveal personal information, like a password or credit card number.

2. Is it correct? Look-alike websites will often include extra letters, numbers instead of letters, or other subtle differences that can be easy to miss.

3. Contact the apparent sender another way. For example, if you get a suspicious email from a company, call them using the number on your bill instead of the phone number in the email, or check their website by entering the address directly in your web browser instead of clicking on a link.

4. Report it as suspicious. Most email providers contain a button for marking spam or suspicious emails which can help flag emails from that sender to other recipients.

Thank you for joining in the #SecureTogether challenge!

Visit action.consumerreports.org/secure_together to comlete the challenge.