USE A STRONG PASSWORD AND A PASSWORD MANAGER

Why It Matters

Strong passwords are your first line of defense against cyber threats. They help protect your data, money, and identity from hackers and malicious actors.

3 STEPS TO STRONGER PASSWORDS

1

Make them long

Aim for at least 16 characters. Longer passwords are harder to crack. Longer is stronger!

2

Make them random

Use a mix of uppercase and lowercase letters, numbers, and symbols *or* create a memorable passphrase using 5-7 unrelated words with creative spelling.

3

Make them unique

Use a different password for every account. Avoid small tweaks to reused passwords — each one should be entirely distinct.

Let a Password Manager Do the Work

A password manager:

- Creates, stores, and fills passwords automatically
- Requires you to remember just one strong master password

We recommend using Keeper, a trusted password manager solution.

FAQ: USE A STRONG PASSWORD AND A PASSWORD MANAGER

1 Why should I use a password manager?

Your password manager will become your favorite tool as you navigate the digital world. With a password manager, you only need to remember one master password to unlock your secure vault of stored passwords.

Benefits of using a password manager

- **Convenience**: No more struggling to remember dozens of passwords.
- **Enhanced security**: Automatically generate and store long, unique, and complex passwords.
- **Time-saving**: Browser extensions and smartphone apps autofill credentials for quick and secure logins.
- **Safe vaults**: You might be wary of storing all your passwords in one place, but high-quality password managers use encryption and zero-knowledge architecture to keep you secure. Password managers are safer than notebooks, sticky notes, spreadsheets, or reusing passwords because you're trying to remember them all.

2 How often should I change my passwords?

If your passwords are already long, unique, and complex, there's no need to change them unless:

- You suspect unauthorized access to your account.
- You receive notification of a data breach involving your account.

Changing passwords too frequently can lead to weaker habits, such as reusing old passwords or creating overly simple ones. Stick with long, strong passwords and update them only when necessary.

3 What about passkeys?

Passkeys are an exciting new technology that remove the need for passwords. Instead of entering a password, with passkeys you typically log in by having a secure device handy (like a phone) and using biometrics, like a facial scan.

APEX technology group

Source: National Cybersecurity Alliance

TURN ON MULTI-FACTOR AUTHENTICATION (MFA)

WHAT IS **MFA?**

A security feature that requires you to verify your identity in multiple ways before accessing an account.

HOW DOES **MFA WORK?**

Enabling MFA means tweaking your login process. First, enter your username and password. Then, verify your identity in a second way.

FOLLOW THESE STEPS

1. Go to **Settings**.
   *It may also be called Account Settings or Settings & Privacy.
2. Look for and **Turn On MFA**
   *It may also be called Two-Factor Authentication or Two-Step Verification.
3. **Confirm.** Select how to provide extra login security.

OPTIONS FOR VERIFICATION

- A text or email with a one-time code.
- A prompt in an authentication app.
- A biometric scan (e.g., fingerprint or facial recognition).
- A physical security key.

WHERE DO I **ENABLE MFA?**

Start by checking the accounts you use daily. Some accounts include: banking, email, social media, and online shopping. If a service offers MFA, turn it on!

Source: National Cybersecurity Alliance

APEX technology group

FAQ: TURN ON MULTI-FACTOR AUTHENTICATION (MFA)

DID YOU KNOW?

Enabling MFA can Prevent 99% of Automated Hacking Attacks

(Microsoft)

WHY BOTHER WITH MFA?

Passwords alone can be stolen or guessed, especially if they are short, use common words, or are reused. MFA makes it harder for cybercriminals to break into your accounts.

CAN MFA BE HACKED?

While MFA is very effective, it's not invincible. Some cybercriminals use social engineering to trick users into granting access. For example, they may flood you with MFA requests, hoping you'll prove one out of frustration or confusion.

WHAT IF I RECEIVE A REQUEST WHEN I'M NOT TRYING TO LOGIN?

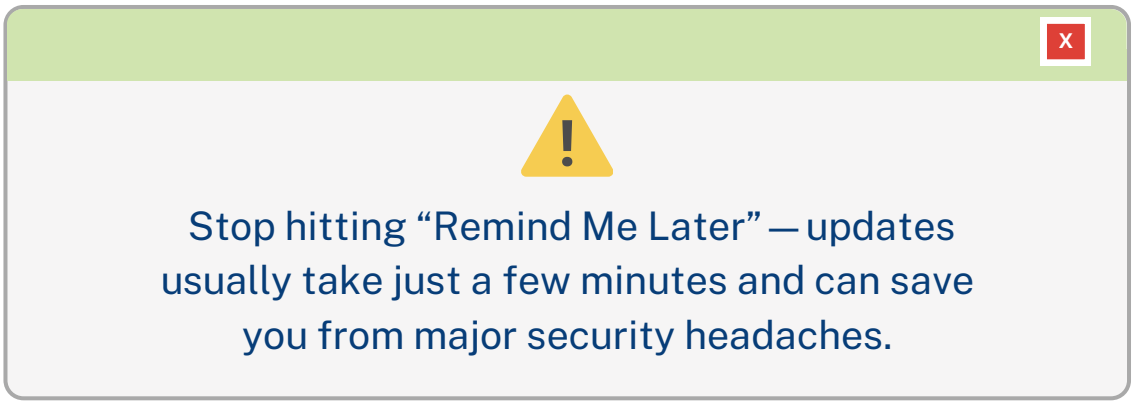
If you receive an MFA request and you aren't logging in, don't approve it. Instead:

- Contact the account's platform immediately.
- Change your password for the account.
- Update any other accounts that use the same password – this is why every password should be unique to the account.

Source: National Cybersecurity Alliance

APEX technology group

KEEP YOUR SOFTWARE UPDATED



Source: National Cybersecurity Alliance

WHY IT MATTERS

- Software updates fix security flaws that hackers can exploit.
- They also improve performance and add new features.

BEST PRACTICES

1. **Turn on automatic updates** in your device settings.
2. **Install updates ASAP** - don’t delay when notified.
3. **Watch for update alerts** - especially for browsers and antivirus software.
4. **Avoid fake update scams** - never click pop-ups or suspicious emails.
5. **Only download updates from trusted sources** - official websites or app stores.
6. **If your device is no longer supported**, consider replacing it or using it offline for non-sensitive tasks.

APEX technology group

SOFTWARE UPDATES: A COMPREHENSIVE GUIDE

OVERVIEW

Keeping software up to date is one of the simplest and most effective ways to protect your devices and personal data.

BEST PRACTICES

Enable Automatic Updates

- Check settings under “Software” or “Security.”
- Search for “Automatic Updates” in your device settings.

Respond to Notifications Promptly

- Not all updates are automatic.
- Install updates for browsers, antivirus, and operating systems ASAP.

Watch for Fake Update Scams

- Close suspicious pop-ups.
- Don’t click on urgent-looking update messages from unknown sources.

Verify Update Sources

- Only update via official app stores or developer websites.
- Never trust pop-ups, emails, or third-party sites.

Make Updates a Habit

- Check settings monthly to ensure updates are working.
- Restart devices when needed to complete updates.

Know When It’s Time to Upgrade

- Unsupported devices are vulnerable.
- Replace or disconnect outdated tech from the internet.
- Avoid using unsupported devices for sensitive tasks like banking.

UPDATES CAN:

Fix malware

Improve performance

Install latest features

APEX technology group

Source: National Cybersecurity Alliance

RECOGNIZE & REPORT PHISHING SCAMS

WHAT ARE PHISHING SCAMS?

Deceptive messages that mimic trusted sources to trick you into revealing sensitive data or installing malware. Recognizing and reporting these scams is essential to protecting yourself and your organization.

HOW TO SPOT A PHISHING EMAIL

- Too-good-to-be-true offers
  - Free money, prices, luxury items
- Urgent or threatening language
  - “Act now!” “Your account will be deleted!”
- Requests for personal info
  - Passwords or financial data
- Unfamiliar attachments or links
  - Hover to preview URLs
- Mismatched sender addresses
  - Slight misspellings or odd domains
- Poor grammar or generic greetings
  - “Dear Customer”

CAUGHT A PHISHING ATTEMPT?

1. Stay calm. Don’t click or reply
2. Report the email
3. Block the sender
4. Delete the email

APEX technology group

Source: National Cybersecurity Alliance

KNOW THE SCAMMER'S PLAYBOOK: RED FLAGS YOU CAN'T IGNORE

RED FLAGS & WARNING SIGNS

The Danger of Urgency: Scammers use urgency to make you act fast — whether it's a fake prize or a threat.

In phishing messages, a sense of urgency can be negative or positive.

- **Examples of positive sense of urgency:** you won a prize, you're owed money, you can get an exclusive deal.
- **Examples of negative sense of urgency:** You've been hacked, the IRS is investigating you, criminals are recording you through your webcam, there is a warrant out for your arrest.

Requests for sensitive information: Legitimate companies and government agencies will never ask for sensitive personal information, such as your password or Social Security number, via email or text.

Suspicious sender addresses or links: Always check the sender's full email address and hover over any embedded links to see the actual URL. Be cautious of domains that are misspelled (e.g., "amazan.com") or use public domains like "@gmail.com".

Unexpected attachments: Avoid opening unsolicited or unexpected attachments, especially from unknown senders. These can contain malware.

APEX technology group

Source: National Cybersecurity Alliance

KNOW THE SCAMMER'S PLAYBOOK: RED FLAGS YOU CAN'T IGNORE

TYPES OF SCAMS OR THREATS

Spear-Phishing

Some phishing emails are personalized using your name, job, or contacts. These are harder to spot but just as dangerous.

Smishing

Phishing that is carried out through SMS text messages.

Vishing

Phishing that uses voice communication, typically a phone call, to deceive victims.

Spoofing

When an attacker impersonates a legitimate person, website, or email address to deceive a victim.

Pharming

A type of cyberattack that redirects users from a legitimate website to a fraudulent one without their knowledge.

Baiting

An attack that lures a victim by promising something desirable for free, such as a movie download or a USB drive left in a public place.

APEX technology group

Source: National Cybersecurity Alliance

SAMPLE PHISHING EMAIL

From: security-alerts@amaz0n-support.com
Subject: Urgent: Your Account Has Been Compromised!

Dear Customer,

We have detected suspicious activity on your Amazon account. Immediate action is required to prevent permanent suspension.

Please verify your account information by clicking the secure link below:

Verify Now

Failure to respond within 24 hours will result in account termination.

Thank you,
Amazon Security Team

WHAT'S WRONG?

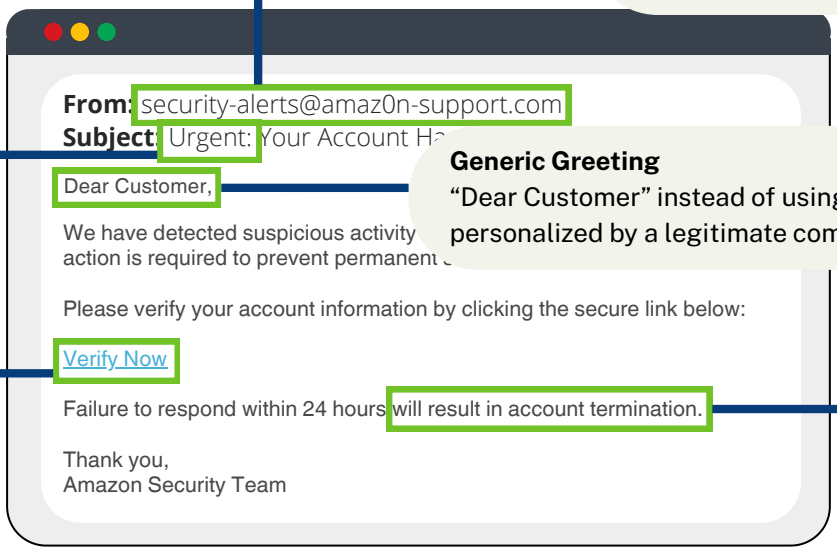
Suspicious Sender Address
"security-alerts@amaz0n-support.com" uses a misspelled domain ("amaz0n" instead of "amazon") and a non-official format.

Urgency & Threats
"Immediate action is required..." and "Failure to respond..." are classic urgency tactics to pressure you into acting without thinking.

Generic Greeting
"Dear Customer" instead of using your name is a sign it's not personalized by a legitimate company.

Fake Link
The link text says "Verify Now," but the actual URL is not Amazon. It's a deceptive domain: secure-login.com with "amaz0n-support" as a subdomain.

Unusual Consequences
Real companies don't threaten account termination over email without prior notice or multiple warnings.



APEX technology group