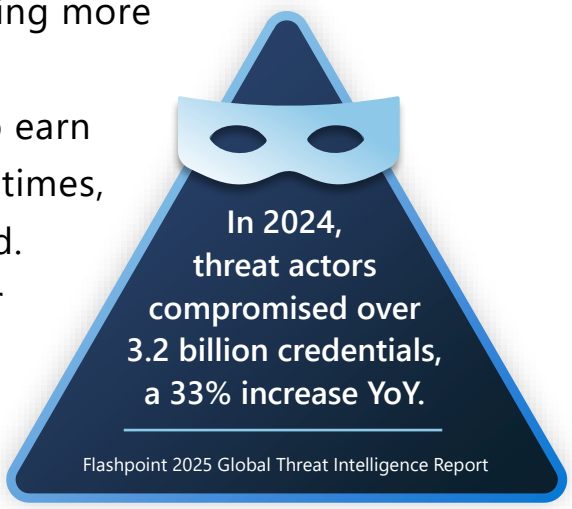
Microsoft Security

CUSTOMER SECURITY MANAGEMENT OFFICE

Identity Protection Guide

Identity-based attacks are rising fast—and getting more sophisticated. These threats often exploit weak passwords and use social engineering tactics to earn your trust and steal data. The worst part? Sometimes, you won't even know you've been compromised. The following best practices will help keep your identity secure.



Critical identity protection practices

Following these identity protection practices at work and at home can reduce your risk of becoming a victim of a cyberattack. To learn more about each practice select the number associated with the practice.

1. Use multifactor authentication (MFA) for all personal accounts
2. Confirm you initiated an MFA request before approving
3. Use a strong and unique password for each account
4. Don't share passwords with others
5. Store passwords using encrypted tools like password managers
6. Regularly check to see if your credentials have been associated with a data breach
7. Immediately change passwords on accounts associated with a breach
8. Pause and ponder before posting on social media to avoid oversharing
9. Don't accept unfamiliar or unsolicited social media requests
10. Regularly review your social media privacy settings to limit access
11. Regularly audit your social media connections to limit access
12. Check for phishing indicators when receiving unsolicited messages
13. Don't contact the sender of a suspicious message
14. Don't select unsubscribe links in unsolicited emails
15. Validate the identity of the sender through official channels before responding to unsolicited messages

Common identity theft tactics

Phishing attacks

Phishing attacks involve tricking users into revealing credentials or approving fake MFA prompts by impersonating trusted people or brands. Threat actors often use social engineering techniques like urgency and too-good-to-be-true offers to get you to engage. These increasingly sophisticated scams account for nearly 80% of breaches, making them the most common entry point for identity theft.

Credential stuffing attacks

Credential stuffing attacks involve the use of giant databases of leaked credentials (combo lists) to automate login attempts across multiple platforms. This method exploits password reuse and scale. With more than 19 billion compromised passwords available online, credential stuffing is a major threat.

Brute-force attacks

Brute-force attacks are a type of cyberattack where a threat actor systematically attempts all possible combinations of password strings, encryption keys, or login credentials until the correct one is found. It's a trial-and-error method that relies on computing power to guess credentials and gain unauthorized access to accounts and data.

Dictionary attacks

Dictionary attacks are a type of brute force attack where an attacker attempts to gain unauthorized access to a system by systematically trying a list of likely passwords—typically words from a dictionary or commonly used passwords like "abcd".

Data aggregation attacks

Data aggregation attacks involve using compiled data from various breaches, social media accounts, and public records to build rich identity profiles. These datasets fuel convincing phishing and impersonation attacks. With AI accelerating this trend, these tactics are becoming faster, smarter, and harder to detect.

Prompt bombing attacks

Prompt bombing attacks entail flooding users with MFA requests, causing frustration and fatigue, and hoping the user will eventually approve one just to stop the distraction. This tactic is now one of the top methods for bypassing MFA.

Identity protection practices

Password practices

1. Use multifactor authentication (MFA) or phish-resistant MFA for all personal accounts

Why it matters

- MFA can help prevent up to 99.9% of attacks.[1]
- If your password is stolen, MFA requires a second verification step, making it much harder for threat actors to gain access to your account.
- MFA helps protect against credential stuffing and data aggregation attacks.

What to do

- Enable MFA on all personal accounts.
- Choose phish-resistant MFA methods (like passkeys) whenever possible over text or push notifications for extra protection.

2. Confirm you initiated an MFA request before approving

Why it matters

- Threat actors often use prompt bombing attacks to trick you into accidentally approving an MFA request.
- One mistakenly accepted MFA request can compromise your identity and data.

What to do

- Pause before approving an MFA request to make sure you did something to trigger the request.
- Immediately change the password for accounts associated with unprompted MFA requests.

3. Use a strong and unique password for each account

Why it matters

- Strong passwords defend against many identity theft tactics, like brute-force, dictionary, and credential stuffing attacks.

[1] Microsoft research study: How effective is multifactor authentication at deterring cyberattacks

- Unique passwords prevent a domino effect—if one account is breached, threat actors can access other accounts using the same credentials leveraging tactics like credential stuffing and data aggregation attacks.

What to do

- Assign unique passwords to every account.
- Follow these guidelines when creating passwords:
  - Include at least 12 characters (but 14 or more is better).
  - Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
  - Don't use a word found in a dictionary or the name of a person, character, product, or organization.
  - Ensure it is significantly different from your previous password.
  - Consider using a memorable phrase, for example: "6MonkeysRLooking^".
- Use a password manager for password creation and password reuse identification.

4. Don't share passwords with others

Why it matters

- Sharing passwords with others, even trusted colleagues or friends, can seriously weaken your security posture.
- The more people who know a password, the greater the chance it will be:
  - Written down or stored insecurely
  - Accidentally shared with someone else
  - Used on an unsecure device

What to do

- Keep your password private, even with trusted coworkers or family members.
- Never share passwords if requested over the phone or in email.

5. Store passwords using encrypted tools like password managers

Why it matters

- Password managers encrypt your data end-to-end, making it hard to unlock in the event of a breach.
- Password managers generate strong, complex passwords for each account, eliminating the need to reuse or remember them.
- Many password managers alert you when credentials appear in a breach and prompt you to update compromised passwords.

What to do

- Choose a password manager that works best for your situation.
- Let the password manager generate and save strong passwords for every account.

Breach practices

6. Regularly check to see if your credentials have been associated with a data breach

Why it matters

- Breaches happen constantly and you aren't always notified promptly, exposing billions of credentials every year.
- Once credentials are leaked, they may be added to combo lists and used in credential stuffing attacks.

What to do

- Use third-party tools like Have I Been Pwned or your password manager's password security check function to see if any of your credentials have been associated with a breach.
- Set a recurring reminder to see if your credentials have been associated with a breach.

7. Immediately change passwords on accounts associated with a breach

Why it matters

- Stolen credentials spread fast. Once a breach occurs, threat actors may quickly use your credentials in credential stuffing or data aggregation attacks.
- Once threat actors access your account, they can:
  - Lock you out
  - Steal personal or financial data
  - Change your recovery options
  - Use your account to target others

What to do

- Immediately change the password for the breached accounts.
- Ensure MFA is enabled on all personal accounts.
- Update all accounts that use the same or similar breached password.
- Replace breached passwords with strong, unique alternatives.

Social media practices

8. Pause and ponder before posting on social media to avoid oversharing

Why it matters

- Threat actors scrape social media for birthdays, job announcements, locations, and personal and professional details. This data helps them create:
  - Convincing phishing attacks using social engineering
  - Fake accounts to pose as you to earn the trust of a friend, family member, or colleague
- Pausing and pondering helps you slow down and focus on the task on hand.

What to do

- Use the "pause, ponder, proceed" approach:
  - **Pause:** Take a moment to consider what is before you, rather than reacting impulsively.
  - **Ponder:** Reflect on the situation, consider doing some research, seek counsel, and evaluate the pros and cons.
  - **Proceed:** Move forward with the decision that feels right after careful consideration.
- Avoid posting birthdays, vacations, or any sensitive information.
- Don't share anything considered confidential on social media.

9. Don't accept unfamiliar or unsolicited social media requests

Why it matters

- With just a few scrolls and some AI magic, threat actors can piece together personal details about you from social media and use the data to conduct data aggregation attacks.

What to do

- Decline requests from unsolicited or unfamiliar people.
- Verify the identity of the requestor through alternative methods before accepting the request.

10. Regularly review your social media privacy settings to limit access to your data

Why it matters

- Threat actors use publicly visible social media profiles, posts, tags, or contacts to create a data aggregation attack.
- Default privacy settings often expose too much.

What to do

- Limit social media profile visibility to trusted "friends" or "connections" wherever possible.
- Revoke social media profile access to third-party apps or tools you no longer use.

11. Regularly audit your social media connections to limit access

Why it matters

- Regularly review your social network connections to ensure only trusted individuals have access to your information.

What to do

- Remove connections you don't recognize or no longer want to have access to your profile and posts.

Phishing prevention practices

12. Check for phishing indicators when receiving an unsolicited message, chat, or phone call

Why it matters

- Phishing techniques have become more advanced, with threat actors rarely make spelling or grammar errors. Instead, they exploit human psychology and emotions to manipulate recipients.

What to do

- Look for signs of social engineering.
- Consider verifying the identity of the sender through alternative methods before engaging.
- If something seems suspicious don't engage and report the suspicious message.

13. Don't contact the sender of a suspicious message

Why it matters

- Engaging with the sender of a suspicious message can inadvertently provide them with more information about you or your organization.
- Responding to a suspicious message can lead to further exploitation.

What to do

- Don't respond to suspicious messages.

14. Don't select unsubscribe links in unsolicited emails

Why it matters

- Clicking "unsubscribe" in a suspicious message may confirm to threat actors that your email is active and monitored.
- Clicking "unsubscribe" in a suspicious message may add you to spam lists, redirect you to a phishing site, or install malware on your device.

What to do

- Use the Report Junk option in your email app (if available) to report the message and block further communications from the sender.

15. Validate the identity of the sender through official channels before responding to unsolicited messages

Why it matters

- Email addresses and names can be easily spoofed. It's easy for threat actors to open accounts or forge sender names or register lookalike domains (e.g., micr0soft.com instead of microsoft.com).

What to do

- Check email addresses carefully for typos or unusual domains.
- Verifying the sender is legitimate through a known, official channel (e.g., Teams, phone call, or company directory).

Secure. Together.

Security is everyone's responsibility – by using this guide and following through on these practices, you play a crucial part in keeping yourself and everyone safe from cyberattacks.

Content in this guide was developed by Microsoft's security education and awareness team with the assistance of Copilot.