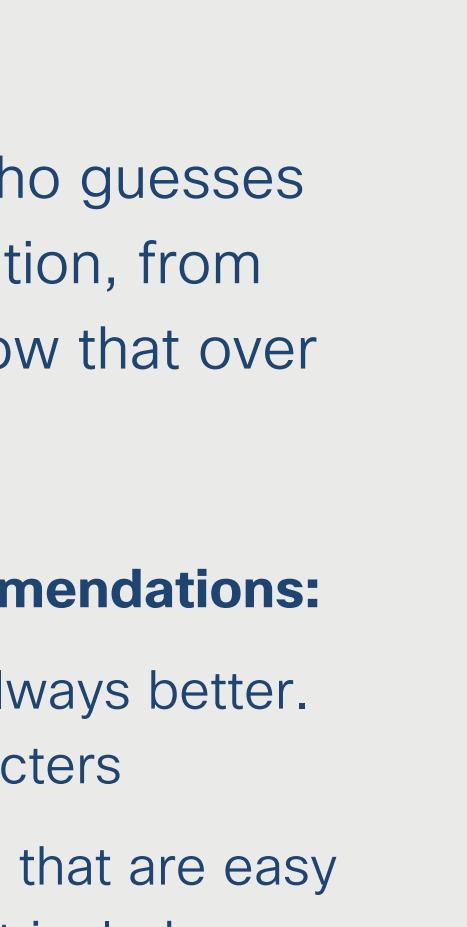


# Top 10 Cyber Tips

**1**

## Keep personal information private

In the wrong hands, your personal information (i.e., date of birth, mother's maiden name, passport ID, etc.), can result in identity theft – and cause havoc to your finances, credit, and mental wellbeing. To learn more about protecting personal data, check out Cisco's [Top 10 Privacy Tips](#).

**2**

## Use caution to avoid bad actors

Bad actors have become more sophisticated and come in all shapes and sizes. Beware of email phishing, text smishing and other social engineering techniques bad actors are integrating into our everyday life. Take a moment to review who is on the other end of your communication before responding.

**When in doubt:**

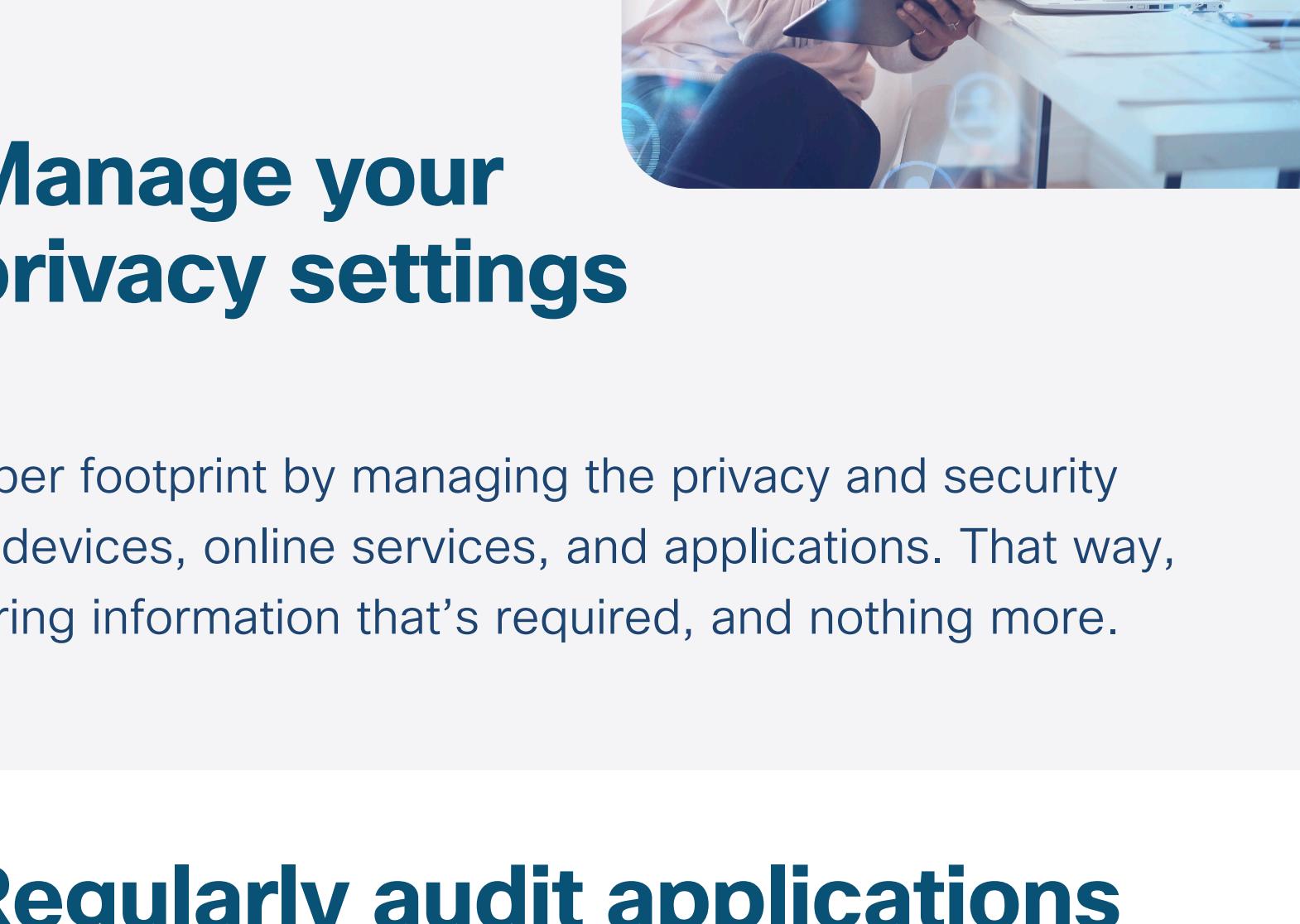
- Check email addresses
- Beware of embedded links or attachments
- Never provide personal information via email or phone
- Go directly to the company's website to follow up on a message instead of replying through an internal link
- Stay vigilant and use caution when asked to do something new, unusual, or different
- Slow down and think carefully before you act

**Bad actors often use:**

- Poor grammar
- A sense of urgency, fear, curiosity, or greed
- Behaviors to gain personal information, including your password
- Deals that are too good to be true
- "Dear sir/madam" and other generic greetings

**3**

## Update software regularly



Bad actors are constantly looking for opportunities in unpatched software. Keep your software up to date—it's one of the most effective security tools you have. Better yet, enable automatic updates, so you never have to think about it.

**4**

## Create strong passwords by using paraphrases



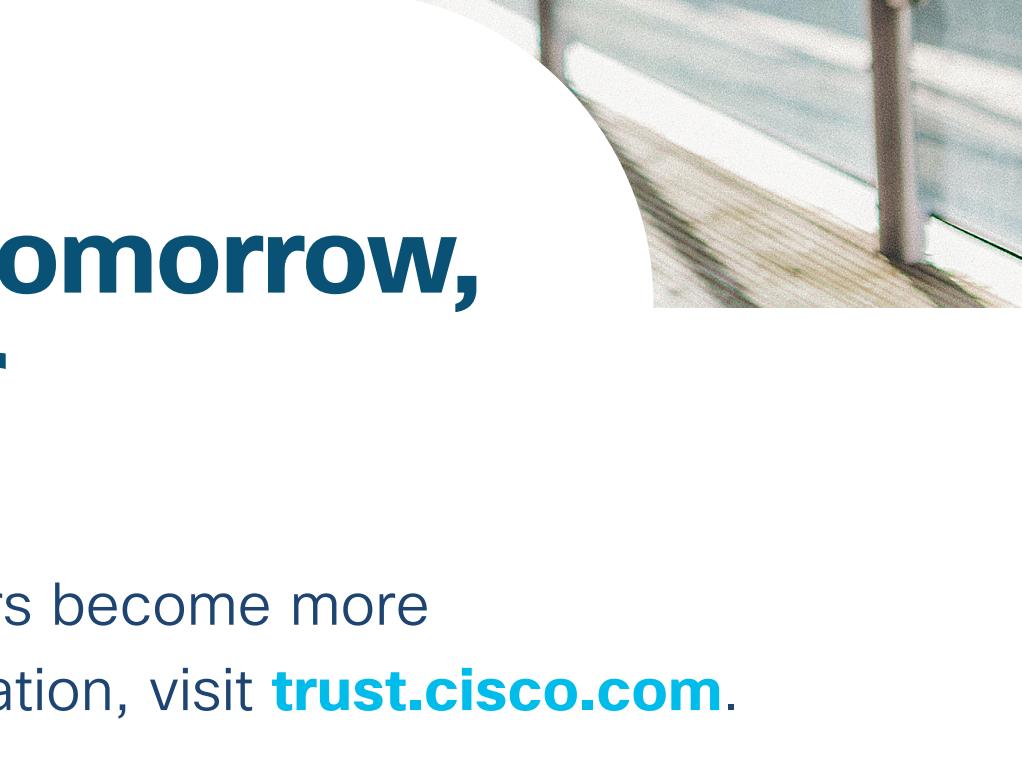
We all have dozens of passwords. Any bad actor who guesses just one can quickly access lots of personal information, from your bank data to your home address. Statistics show that over **280,000 passwords are stolen each day!**

**Strong password recommendations:**

- Longer passwords are always better. Aim for at least 14 characters
- Choose unusual phrases that are easy for you to remember that include numbers and symbols
- Never use the same password for multiple accounts
- For best results, use a password manager to create and store passwords

**5**

## Use two-step verification whenever possible



Two-step verification, also known as multifactor authentication (MFA) or two-factor authentication, strengthens security by requiring additional ways to verify your identity beyond your user ID and password. These added layers help guard against phishing, social engineering, and password brute force attacks.

**6**

## Be cautious of free Wi-Fi



Bad actors can hack free or public Wi-Fi to discover the websites you're visiting and capture the information – including personal information – that you send over the network. [Learn more about Wi-Fi attacks](#) and how to protect yourself from them.

**If you must use free Wi-Fi, avoid websites that use and retain your personal data:**

- Online banking
- School accounts
- Social media

**7**

## Don't leave a cyber footprint on shared or public devices



When using a public computer or any device that is not your own, another user may be able to access your data and accounts.

**Before signing off, make sure you:**

- Disable any options to "save passwords"
- Log out of your accounts when finished
- Delete cookies, cache and browsing history

**8**

## Manage your privacy settings



Secure your cyber footprint by managing the privacy and security setting on your devices, online services, and applications. That way, you're only sharing information that's required, and nothing more.

**9**

## Regularly audit applications you have installed as privacy settings can change with upgrades



Some mobile apps may have access to more information than you realize. Before downloading a new app, pay close attention to the permissions it requires.

**Do you really want that app to capture data from your:**

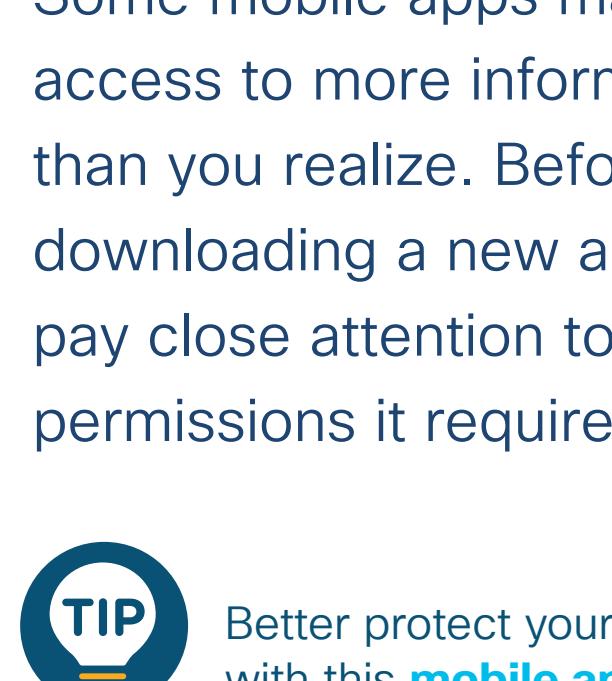
- Camera roll
- Microphone
- Keystrokes

**10**

## Secure tomorrow, together



Share your knowledge to help others become more Cisco cyber-solid. For more information, visit [trust.cisco.com](#).



© 2021 Cisco and/or its affiliates. All rights reserved.

