ePAPER

APCI FEDERAL CREDIT UNION

Think Before You Share Online

Consider what you post

Where to Start

Online activity has become a regular part of daily life. We watch and create content, post photos and videos, play games, and share updates with friends and family online. However, risks come with what we share as every encounter may not be genuine.

The most effective tools to staying safe online are critical thinking and patience. Taking a moment to pause and evaluate a situation can help protect you, your accounts, your devices, and those around you. Without these tools you may unintentionally overshare, leading to embarrassment, harm, or misrepresentation. Below are a few things to keep in mind before you share online.

Your audience is larger than you think. Privacy settings do not guarantee control over your content. Once shared, any photo, video, or message can be captured and redistributed. Before posting, ask yourself if you would be comfortable sharing the content with someone in person.

Respect the privacy of others. Content often includes more than just yourself. Sharing photos or videos without consent can be intrusive, inappropriate, or even unsafe. Always ask permission before posting. If the answer is no, do not post.

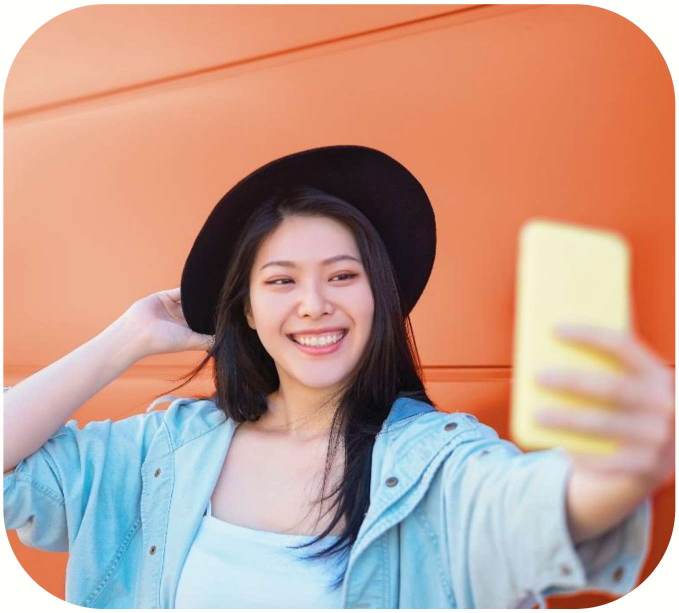
Once posted, it cannot be taken back. Even if you delete content or rely on apps with expiration features, your content may still be saved, copied, or circulated indefinitely.

Practice Courtesy Online

Professionalism and courtesy are as important online as they are in person. Without tone of voice, facial expressions, or body language, digital communication can be easily misinterpreted.

Communicate thoughtfully. Treat online and in-person interactions with the same consideration.

Slow down. Before sending a message ask yourself, “How might this message be received?”



Consider other perspectives. There is a real person behind another account’s photo or avatar. You should always consider the perspectives and feelings of others.

Be mindful of tone. Avoid using all caps, excessive punctuation, or oversized fonts. These could appear aggressive depending on the context of the messaging.

Share responsibly. Before sending a message or posting content, consider if it is necessary to share the information.

Be honest. Creating accounts that appear to be another individual is dishonest and can be harmful. Impersonation can damage reputations, create conflict, and undermine trust.

Address Cyberbullying

Everyone deserves to feel safe, both online and in person. Bullying takes many forms, including hurtful comments, offensive images or memes, or harassing private messages.

If you are a target of cyberbullying, do not engage. Instead, document the behavior and seek help from adults, professionals, or law enforcement.

If you witness cyberbullying, be an upstander. An upstander is someone who speaks up, intervenes, or supports the person being targeted.

Protect Your Privacy

Every online action leaves a digital footprint. Consider the following steps to make sure your footprints do not lead to sharing information that you did not intend to.

Adjust privacy settings. Review privacy controls on devices, apps, and social media accounts to manage who can view your content and connect with you.

Manage location sharing. Disable location features when unnecessary. Consider when it is safe to share your location. For example, if you are traveling and no one is staying at your house, consider waiting to post about your trip until you return.

Limit online connections. Keep your online connections to individuals you know personally. While interacting through text, social media, or online gaming can be enjoyable, it is important to remember that everyone is not who they claim to be.

Protect Your Information

Once personal details such as your Social Security number, passwords, or financial account information are shared, they cannot be retrieved. Safeguard your data with the following practices.

Do not respond to suspicious requests. Avoid replying to messages that ask for personal information, even if they appear to come from a friend, family member, or legitimate organization. These messages are often fraudulent attempts to steal your information. Report any suspicious messages.

Check app permissions. Before downloading an application, check what data and features it has access to. Be cautious of apps that request unnecessary permissions.

Review in-app purchases. Understand purchase details before completing transactions. When using a shared or family account, confirm you have permission before making the purchase.

Protect Your Accounts

Your online accounts hold significant amounts of personal information. Below are steps to strengthen the security of your accounts.

Create strong passwords. Choose passwords that are at least twelve characters long and include a combination of upper and lower letters, numbers, and symbols.

Do not reuse passwords. Create unique passwords for each account. This prevents one compromised password from granting access to multiple accounts.

Keep passwords private. Do not share any of your passwords with friends, family, or significant others.

Be strategic with security questions. Choose questions that only you can answer. Try to avoid using answers that can easily be found online.

Enable multi-factor authentication (MFA). MFA adds an additional layer of protection by requiring something beyond a password, such as a verification code sent to your device.

Change Passwords Promptly. If a company reports a data breach that may have exposed your login credentials, change your password for that account immediately.

Protect your devices

Keeping your devices secure is essential for safe and enjoyable online activity. The following tips will help to keep your devices protected:

- Keep software up to date to defend against the latest threats.
- Do not click links or open attachments in unexpected emails, texts, or messages. Links and attachments could contain malware or spyware designed to compromise your device.
- Use strong passwords or biometric authentication to prevent unauthorized access to your photos, messages, and accounts.
- Do not leave your phones, tablets, or laptops unattended in public spaces. Keep devices in a safe place when not in use.