SECURITY-MINDED

Practical security wisdom for daily life.

ARE YOU SHARING WITH SCAMMERS?

Unsafe social media habits give cyber criminals exactly what they want

Sharing on social networks can feel like a lively conversation among friends, family, and colleagues. That's what makes it so useful—and fun! Unfortunately, scammers also use social networks, gathering personal information that helps them steal identities, compromise accounts, or send highly targeted phishing emails.

Should You Share?

The moment you share something online, you lose control over how it might be used. Anyone could see it.

Imagine you're at a restaurant with friends or family. Perhaps you talk about politics, your upcoming vacation plans, or interesting news at your job. Now, imagine that a criminal has been sitting at the next table the whole time, recording every seemingly insignificant remark. Is there a chance you've shared information that could harm you or your organization?

Scammers often sift through social network profiles, piecing together information to attack people and organizations. They also use innocent-looking quizzes or surveys to collect information without arousing suspicions. Avoid the temptation to fill in a quiz or survey, no matter how many of your connections have shared it or tagged you in it.

Check Before You Connect

Accepting a scammer's connection request puts your information at risk. Your other connections might assume the connection is someone you trust, which puts their data at risk, too. It's safest to not accept a social network connection until you're certain you know and trust the person.

If a stranger asks to connect:

- Consider why he or she wants to connect. Do you have mutual connections or belong to the same professional networks?
- Ask mutual acquaintances for details or search online to confirm the person's identity.

Scammers might try to connect by creating fake profiles that impersonate people familiar to you. If you receive a request from someone you're already connected to, it could be a scam. Always confirm duplicate requests with your existing connection. Immediately remove anyone from your network if their behavior seems suspicious.

What Can I Do?

- **Set limits** – Limit the amount of information you share and the number of people you share it with. Make sure you know and trust connections before sharing information or agreeing to meet them.

Is there a chance you've shared information that could harm you or your organization?

TIPS FOR FAMILY AND FRIENDS

Share these social networking tips with the people in your life:

- **Think before you share –** Could sharing this comment, photo, or link potentially harm you personally or professionally, either today or in the future?
- **Privacy settings aren't foolproof –** You may intend to only share your thoughts with a small circle of online friends and followers, but they can have an impact far beyond. If you wouldn't say it to or share it with a stranger, it probably shouldn't be posted on social media.
- **Watch out for imposters –** Accepting a stranger's connection request can give cyber criminals access to your profile. Scammers might also create fake profiles to impersonate people familiar to you.
- **Protect your login credentials** – Use strong authentication methods for each account. If the social network requires security questions, consider using fake answers that don't match anything you've posted. It's easy for a scammer to find out your mother's maiden name or the names of your schools, pets, and childhood friends.
- **Use privacy controls** – Regularly review your privacy settings and permissions for updates—but be aware of their limitations. Determined scammers can bypass these controls, and there's always a chance you could unknowingly share or allow access to your information.
- **Use caution with third-party apps** – Logging into an app with your social network account gives that app some level of access to your information and connections. Make sure you carefully examine and verify all third-party apps. Using fewer apps also helps reduce your risk.

What If My Account Is Compromised?

Act quickly to reduce risks to you, your connections, and your organization. Immediately change your password and check your other account settings for unexpected changes. Use another communication method, like email, to notify your social network provider and all of your connections.

You can learn more about safe social networking in your organization's security awareness training.

Activity Corner // Logic Puzzle

Imagine you're on your favorite social networking site and see that a few of your friends have taken an online personality survey. It seems like a fun way to compare birthdays, alma maters, and other milestones. But that information could end up in the wrong hands—even if the quizzes are taken anonymously. How much could scammers learn by browsing through these quizzes?

Directions: Use the list of clues and the grid below to determine when each person was born and what college they attended. Each person is matched to only one school, and no two people have the same birthday.

CLUES:

1. **Matt was born on October 8.**
2. **Amy has a birthday sometime after the Auburn University graduate.**
3. **The four people include the person born on January 15, Matt, Susan, and the University of Virginia graduate.**
4. **The person whose birthday is on July 22 is either Matt or the graduate of Texas Tech.**

	Joe	Amy	Matt	Susan	Michigan State	Texas Tech	Auburn	Virginia
Jan. 15								
Apr. 12								
Jul. 22								
Oct. 8								
Michigan State								
Texas Tech								
Auburn								
Virginia								

Answers: 1. Joe; January 15; Auburn University 2. Amy; April 12; University of Virginia 3. Matt; October 8; Michigan State 4. Susan; July 22; Texas Tech