

NEWSLETTER



Staying safe online is just as important as staying safe in the real world. In this edition, we're talking about cyber security and how to protect yourself from scams and fraud. You'll learn tips to keep your personal information safe, how to spot suspicious activity, and what to do if something doesn't seem right.

Technology is awesome—you can chat with friends, play games, shop, and even manage money with just a few clicks. But with all those opportunities comes the need to be careful. Scammers are always looking for tricks to get personal information, like passwords or account details.

We'll share simple tips for creating strong passwords, spotting suspicious ads, and knowing what to do if you ever feel like something online isn't quite right. The more you know, the safer you'll be!

— Your Friends at LLCU

ASK LLCU

Send us a question you have about banking, money, or working at a credit union! If your question is selected an LLCU staff member will answer it here!



ANSWERED BY:
Colin St. Michael
Teller
Mattoon

What is a PIN number used for?

This question was submitted by Sam in Bloomington, IL.

PIN is short for Personal Identification Number. It's a secret number just for you. When you get a debit card, you choose a PIN to keep the card safe. It's four digits you pick that you will not forget.

The very first debit card was used in 1972 in London, England. John Shepherd-Barron, the inventor of the ATM (Automated Teller Machine), thought a PIN should be six digits. His wife said she could only remember four, and that became the common size of PIN. When you want to take money out of an ATM, you put your debit card in and type your PIN. Since that number is your secret, no one else can take money out of your bank account. Even if someone has your debit card, they cannot use it without your PIN. You might think it would be easy

to guess four digits, but there are actually 10,000 possible combinations you can make with four digits. It's a short number, but it's a safe number.

The PIN is getting used for more than just ATMs. Smartphones, desktop computers, laptops, and software now use a PIN for security. At some stores, you can use your debit card to buy something and, after you put in your PIN, it will let you get cash back to save you a trip to the ATM.

Some technology devices are using BIOMETRICS in addition to or instead of a PIN. This is when you see the option to use Face ID or Fingerprint. Look for more information about Biometrics in next month's newsletter.

CHLOE AND SAFETY SAM'S WILD WEST ADVENTURE

Chloe was playing on her laptop one sunny afternoon when a pop-up for her favorite game flashed: “Free Coins!”

“Wow, free coins!” she exclaimed. But her cat, Luna, gave a worried meow and hopped off her lap. Just then, the screen flickered, and a padlock-shaped sheriff in a cowboy hat appeared.

“Howdy, Chloe! I’m Safety Sam, sheriff of the internet frontier,” he said with a tip of his hat. “That pop-up’s as tricky as a snake-oil salesman. Let me show you how to ride safe through the Wild West Web.”

With a whirl of dust, Chloe suddenly found herself in a busy Old West town—horses at the hitching posts, tumbleweeds rolling by, and a wooden saloon swinging open its doors.

Be Careful with Pop-Ups

A “Free Coins!” poster tumbled across the street like a loose wagon wheel.

“Pop-ups can trick you into danger,” Safety Sam warned.

“Never click ones you don’t recognize or seem too good to be true—they might steal your info.”

“Got it—no random pop-ups!” Chloe said firmly.

Use Strong Passwords

At the sheriff’s office, Safety Sam pointed to a heavy iron key hanging on the wall.

“Your password is your key to the town credit union,” he explained. “If it’s weak, bandits can bust in. Make it strong with letters, numbers, and symbols.”

“Like ‘Cowb0y!Boot\$4’” Chloe offered.

“Perfect, partner!” said Safety Sam with a grin.

Always Ask an Adult

By the town well stood a wooden sign that read *TELL AN ADULT!*

“If someone online begins asking personal questions, don’t

answer and always tell a trusted adult,” Safety Sam said.

“What if someone online wants to meet me?” Chloe asked.

“That’s a red flag bigger than a rodeo banner! Never meet strangers online—tell your parents right away.”

Keep Personal Info Private

Inside the saloon, Chloe noticed outlaw posters listing names and addresses.

“See how dangerous it is when the wrong folks know too much?” Safety Sam said. “Online, never share where you live, your school, details about your family, or other private details.”

“No posting pictures of my house, then,” Chloe nodded.

“Exactly,” Safety Sam said, giving her a thumbs-up.

Always Log Out

Finally, they walked to the train station at the edge of town. A glowing sign over the platform read *LOG OUT*.

“When you’re done online, always log out—especially on a shared computer,” Safety Sam explained.

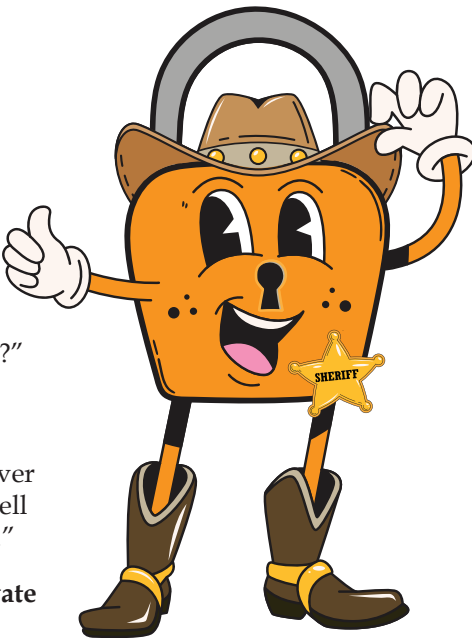
“Like at my friend’s house?” Chloe asked.

“Exactly right,” said Safety Sam.

With a blink, Chloe was back at her desk, Luna curled up on her lap.

“Thanks, Safety Sam! I’ll be extra careful online from now on.”

Luna gave a happy purr, and Chloe smiled, ready for safe adventures—on the frontier and online.



Dollars & Dreams: Finance Skills for Teens

Spotting Scams: Protect Yourself and Your Money

Being a teen today means you’re probably spending more time online than ever—shopping, gaming, streaming, or just hanging out on social media. Unfortunately, scammers know this too. Fraud isn’t just something that happens to adults—teens are often targeted because scammers think they can trick you more easily. The good news? With a little awareness, you can protect yourself and your money.

Common Scams Teens Face

- Phishing Messages – Emails, texts, or DMs that look official but are really fake. They often ask you to “click here” or “verify your account.”
- Fake Online Shopping Deals – That unbelievable sneaker price or “limited edition” item? If it seems too good to be true, it usually is.
- Prize or Contest Scams – Scammers may say you’ve won money or a gift card, but first they need your personal or payment info.
 - Job Scams – Offers that promise quick cash for little work can be a setup to steal your identity or money.



How to Protect Yourself

- Think Before You Click – Don’t open links or download attachments from unknown people.
- Use Strong Passwords – And don’t reuse the same password everywhere.

- If using Biometrics (Face ID or fingerprint) is an option, it’s always best to use that over a passcode. Also, use Multifactor Authentication, which is when you can receive a text with a security code.
- Keep Personal Info Private – Never share your account numbers, debit card details, or even your full birthday with strangers online.
- Keep Phone and Computer Software up to date, as well as anti-virus programs, to ensure your devices stay safe from malware and viruses.
- Check Before You Buy – Shop only on trusted websites and read reviews before making a purchase.

What To Do If It Happens

Even when you’re careful, mistakes happen—and that’s okay. What’s important is acting quickly:

1. Tell someone you trust right away, like a parent or guardian.
2. Contact your credit union so we can help protect your account and stop any suspicious activity.
3. Change your passwords on all accounts immediately.
4. Report the scam to the platform where it happened (social media site, marketplace, etc.).

Final Tip

Remember: your money and your identity are valuable. Scammers are counting on you not paying attention—but now you know what to look for. Stay alert, ask questions, and know that your credit union is always here to help if something doesn’t seem right.

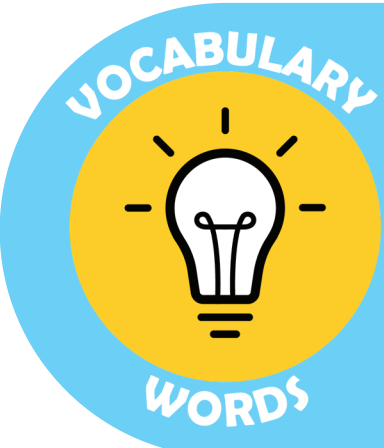
How to Build a Strong Password

Your password is like the code to your locker—it keeps your stuff safe! A weak password (like 1234 or password) is super easy for someone to guess. A strong password is harder to crack, but still easy for you to remember. Here’s how to build one:

- Make it at least 8 characters long (longer = stronger).
- Mix it up with letters, numbers, and symbols (!, #, \$). Some sites even allow you to add spaces into your passwords!
- Don’t use obvious things like your name, birthday, or pet’s name.
- Try combining two random words with numbers and symbols. Example: Rocket!Pizza27

Pro Tip: Using a favorite song lyric as a password can make the password easier for you to remember but harder to guess! Level up by adding a combination of special characters and numbers into it.

Remember: you should not use the same password for all your accounts. Come up with several combinations that you can remember.

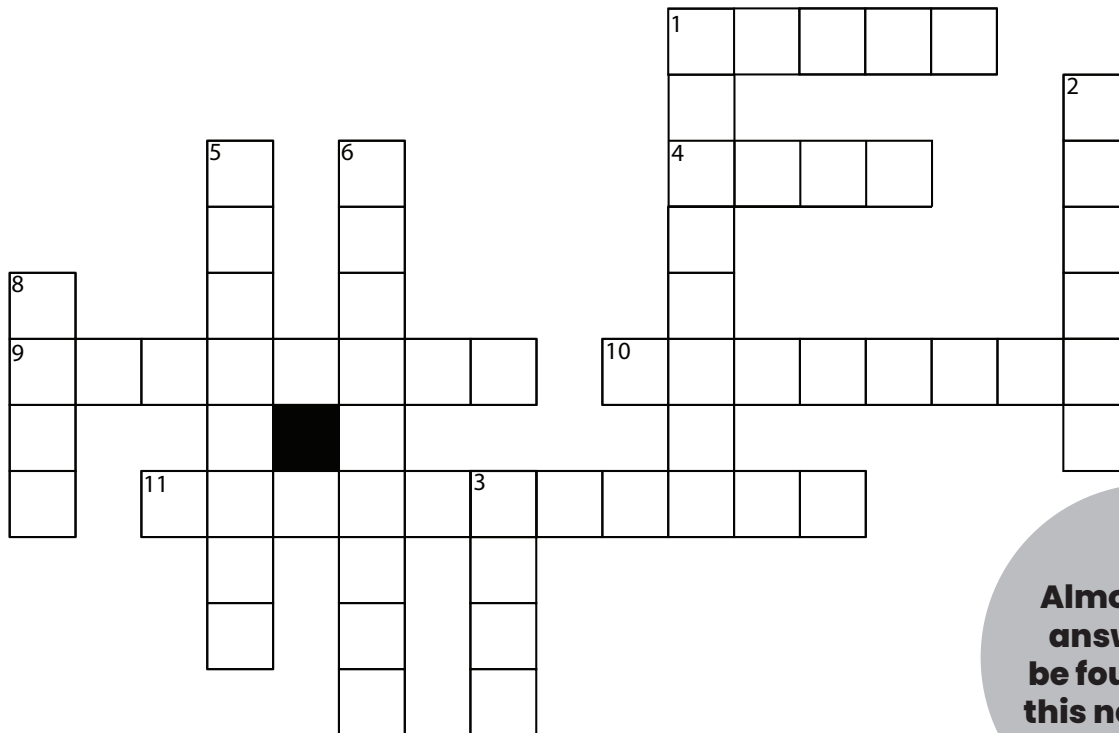


Password	A secret word or mix of letters, numbers, and symbols you use to get into your accounts. It’s like the key to your online “house.”
Pop-Up	A small window that suddenly shows up on your screen, often trying to get you to click it. Some are safe, but many can be tricks.
Private Information	Personal details about you, like your name, address, school, or phone number. You should keep these safe and not share them online.
Stranger Online	Someone you don’t really know in real life. Even if they seem friendly in a game or chat, you should be careful and not share personal info with them.



Cyber Safety Crossword

Bring the completed crossword into your nearest LLCU branch to get a prize from the treasure box.
Ask an adult for help or visit a branch to ask an LLCU Rep!



**Almost all the
answers can
be found inside
this newsletter!**

ACROSS

1. A small window that suddenly shows up on your screen, often trying to get you to click it.
4. A trick to steal your money or information online.
9. A fake email or message that tries to trick you into sharing personal information.
10. Keep this updated to stay safe on phones and computers.
11. Be careful what you post here - friends and strangers can see it.

DOWN

1. You should make this hard to guess with special characters and numbers.
2. A bad person online who tries to trick you.
3. Always ask a parent before clicking on a strange _____.
5. A secret word you type to get into your account.
6. A program that protects your computer from viruses.
8. A place where your emails go if they look suspicious.