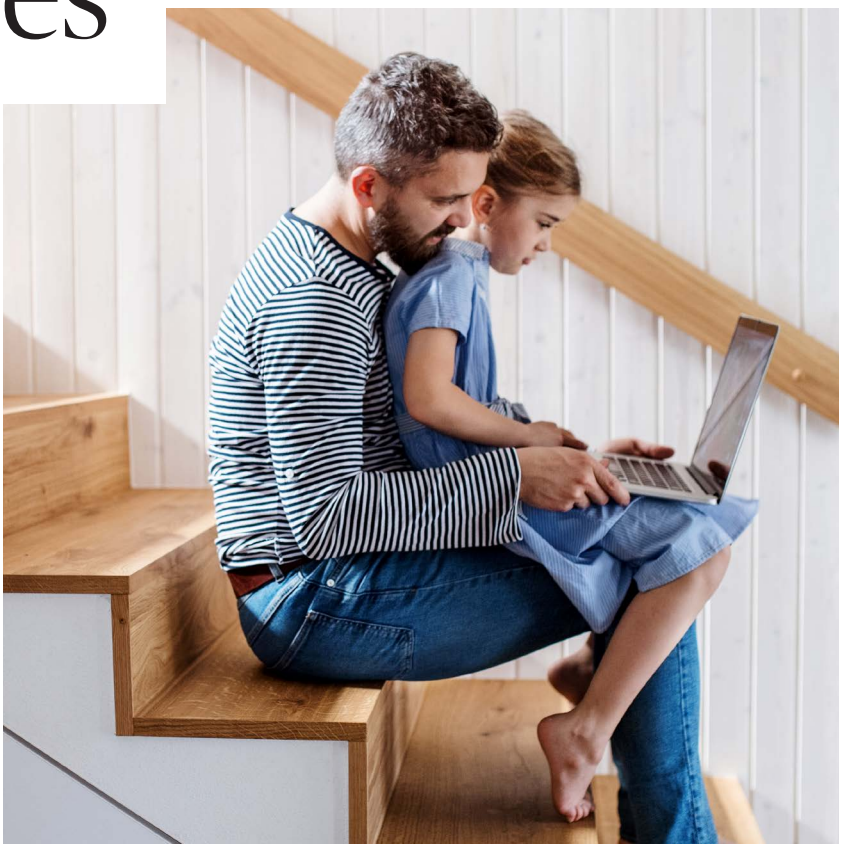
Lincoln Financial Group®

RETIREMENT PLAN SERVICES

Overview

Digital finances, cybersecurity, and kids

Teach your kids how to manage and protect their digital finances



Our kids' lives are intertwined with technology, so it's no surprise that they prefer to spend money and bank online. But before they venture into the digital world of finance, you have a chance to teach them how to do it safely and wisely.

Help them understand

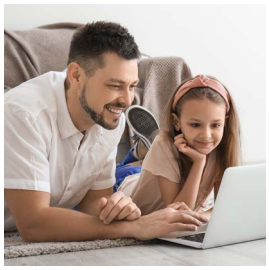
Kids go online at younger and younger ages, and even the youngest want to make in-app purchases. That means it's never too early to start teaching your children about digital money. Most kids can understand the concept of money by age five, but you know your child best. Here are some tips to help them understand that real and virtual money have the same value:

Use real money first.

To make the lessons real, it's best to have young children use cash and coins first before introducing the concept of digital money.

Take a trip to a bank.

If they have an allowance or birthday money, you can open a savings account and deposit their savings.



Set up digital access.

Once they've opened an account, you can help them register for online access. Show them the deposits they made at the bank — seeing their deposit online can help them make the connection between real and digital money. Help them make regular deposits until they understand that their real money and virtual money are the same.

Help teens and tweens be smart online consumers

60% of people

plan to use digital payments in the future and nearly a third want paper money and coins phased out[1]

Following influencers, constantly seeing ads pop up on websites, and noticing trends on social media, teens and tweens today are often one click away from an impulse purchase. Now's the time to start the conversation with your kids about managing their money in a digital world.

The same rules apply to online shopping as they do to going to the mall. Have a conversation about financial basics — needs versus wants, how to budget, and how to save a portion of their earnings. You'll also want to make sure they understand these digital payment options so there are no surprises when the bill comes or they check their account balance:

Credit cards

Credit cards operate with a line of credit, typically tied to a bank. When they're used, money is borrowed from the bank and billed on a monthly basis. If the whole balance isn't paid, the bank will charge interest, which can be as high as 20%. If a kid can't afford their credit card balance, they'll be paying more than sticker price for their purchases. For example, if the card has a 20% interest rate, and they owe $1,000 but only pay $100, they'll pay an extra $180 in interest on the balance.

Debit cards

Debit cards act more like cash with the money deducted immediately from a bank account when used. Some debit card purchases are free, but some can have extra fees. You can find debit cards for kids that allow parents to set limits.

Mobile payments

Mobile payments allow kids to pay for purchases through an app on their phone or tablet. Unlike credit or debit cards, they often allow person-to-person payments.

[1]"New Research: Consumers Want Contactless and Digital Payments Due to COVID-19," Rapyd, August 11, 2020, https://www.rapyd.net/blog/contactless-and-digital-payments/.

Teach your kids about cybersecurity

Cashless payments and online banking make buying and saving easy and convenient. It's no wonder their popularity is growing. But just as you babyproofed your home and gave them safety lessons when they were young, you need to set up online safeguards and parental controls to protect your kids and teach them how to avoid the hidden dangers. Familiarize yourself with the threats, then teach your kids how to defend against them.

95% of cybersecurity breaches are due to human error[2]

A hacker attack occurs every **39 seconds**[2]

[2]Milkovich, Devon, "15 Alarming Cyber Security Facts and Stats," Cybint, December 23, 2020, https://www.cybintsolutions.com/cyber-security-facts-stats/.

Know the threats

Types of threats	Defense skills to teach kids
Phishing. These scams involve a variety of methods, such as an email or social media message, that lure you into clicking a link so your personal information can be collected.	▪ Spot the fakes by hovering the mouse over the link to see if the URL address is different than the sender. ▪ Never open email links from unknown sources. ▪ Question anyone offering money or job opportunities.
Identity theft. When someone uses your personal information to commit fraud or other crimes.	▪ Provide only the required information to set up a social media or other type of account. ▪ Use web browser privacy settings to keep names and email addresses private. ▪ Keep cellphones locked and don't leave them unattended.
Weak passwords. If your password isn't strong enough, you increase the risk that your personal information can be stolen.	▪ Create unique passwords for each account using a combination of upper- and lowercase letters, numbers, and symbols. ▪ Use two-factor authentication when available for an extra layer of security. ▪ Never share passwords with friends.
Public Wi-Fi. Public networks, such as the ones at coffee shops or the mall, aren't as safe as private ones.	▪ Use private, secure networks. ▪ Run antivirus software and software updates.
Unsecure websites. Look for signs of encryption before buying anything online or personal information could end up in the wrong hands.	▪ Shop at sites that begin with "https." The "s" stands for secure and means that the merchant encrypts your password, credit card numbers, and other information to protect them. ▪ Look for a lock symbol in the web address, which means that only the website owner will see your information.
Protect your home computer. Just as you lock the doors on your house, you need to make sure your computer doesn't let in any unwanted intruders.	▪ Password protect your home router and use the encryption feature to keep personal information safe. ▪ Use web browsers that allow web browser blacklisting, which prevents you from visiting untrusted sites. ▪ Limit allowing cookies to only the sites that require it.

If you'd like more information about managing digital finances or cybersecurity, consider speaking to a financial professional.

Not a deposit
Not FDIC-insured
Not insured by any federal government agency
Not guaranteed by any bank or savings association
May go down in value

LincolnFinancial.com/Retirement

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates.

Affiliates are separately responsible for their own financial and contractual obligations.

LCN-3477343-030321
POD 3/21 **Z01**
Order code: DC-CYBER-BRC002

Lincoln Financial Group®