NOTES FOR TEACHERS

The Seed Phrase

Students learn what a seed phrase is: 12 or 24 words that act as one backup for every key in a wallet. A lost phone doesn't mean lost coins, but anyone who gets the words can take them, so the words stay offline and are never typed into a website or sent to anyone.

Grades 9–12 | **1:37 video** | **Managing Risk 12-11c** | **Free to use, no sign-up**

STEP 1

Before watching

> If you lost your phone today, what would be gone for good, and what could you get back? How would you get it back?

STEP 2

Watch the episode

Bitcoin Basics, 1:37: thesteadyblock.com/episodes/seed-phrase/ (also on YouTube, @TheSteadyBlock)

STEP 3

Discussion questions

1. Max's phone sank to the bottom of a lake, but his coins were fine. Why? What did he need to get them back, and what didn't he need?
2. Why do scammers go after the words instead of trying to break into the wallet some other way? Name the tricks from the episode and one way to spot each.
3. Supporters say a backup you keep yourself means no company can lose or lock your coins; critics say it puts everything on one piece of paper that can be lost, stolen or found, which is a lot to ask of most people. Where would you keep a backup like this, and who, if anyone, should know where it is?

STEP 4

Exit quiz

1. What is a seed phrase?

A. A password the wallet company can reset for you
B. A code that only works in one app
C. The name of your bitcoin address
D. 12 or 24 words that can rebuild every key in your wallet

2. Max's phone, wallet app and all, sank in a lake. What happens to his coins?

A. They are still on the shared record, and his 12 words can bring back the keys
B. They sank with the phone
C. They go back to whoever sent them
D. The wallet company keeps them until he proves who he is

3. The words in a seed phrase are picked at random from a standard list. How many words are on that list?

A. 12
B. 24
C. 2,048
D. 1 million

4. A pop-up says your wallet is at risk and asks you to type your 12 words to "verify" it. What should you do?

A. Type them quickly so you don't lose your coins
B. Close it: it's a trap
C. Send them to support in a chat instead
D. Type only the first six words

5. Where does the episode say to keep your seed phrase?

A. In a photo on your phone
B. In an email to yourself
C. Written down and kept offline, somewhere safe
D. With a support agent, for safekeeping

Key terms

Seed phrase	12 or 24 words that spell out one secret number; a wallet can rebuild every key from them. Also called a recovery phrase.
Restore	Typing the seed phrase into your own wallet app to bring back the same keys, for example on a new phone.
Offline	Not stored on any device connected to the internet, such as words written on paper.
Phishing	Tricking someone into handing over secret information, for example with a fake support chat, a fake app or a pop-up.

National standard

MAIN STANDARD · MANAGING RISK 12-11C

Recommend strategies to reduce the risk of identity theft and financial fraud.

Part of standard Managing Risk 12-11: “Online transactions and failure to safeguard personal documents can make consumers vulnerable to privacy infringement, identity theft, and fraud.”

MANAGING RISK 12-11A

Provide examples of how online behavior, e-mail and text-message scams, telemarketers, and other methods make consumers vulnerable to privacy infringement, identity theft, and fraud.

MANAGING RISK 8-7B

List actions that an individual can take to protect personal identification information.

The episode’s rule (write the words down, keep them offline, never type them into a website or send them to anyone) is a fraud-prevention strategy students can recommend (12-11c), and its fake support chats, fake wallet apps and pop-ups are examples of how online scams target people (12-11a).

From the National Standards for Personal Financial Education (Council for Economic Education and Jump$tart Coalition, 2021), Managing Risk grade 12, p. 40; Managing Risk grade 8, p. 38.

Numbers in this episode

As of October 2026

- 12 or 24: Words in a wallet’s backup (the BIP39 standard also allows 15, 18 and 21). Twelve words carry 128 random bits plus a short checksum; 24 words carry 256 bits.
- 2,048 words: The standard English word list, from “abandon” to “zoo”. The first four letters of each word are enough to tell it apart.
- 1 backup: The words are turned into a seed, and the wallet derives every key from that one seed (BIP32), so the same words always rebuild the same keys.

- 3.4 × 10^38: Possible 12-word phrases (2^128). Guessing someone's words by chance is as hopeless as guessing a key.
- 0 requests: Police, governments, banks, wallet providers and real support teams will not ask you to send your recovery words by email, text, social media, online form or letter (Canadian Anti-Fraud Centre, Aug 2026).

Where each number comes from is listed on the episode page.

Further reading

For students or teachers who want to go deeper.

FOR STUDENTS **CAFC Bulletin: Cryptocurrency Wallet Fraud** (https://fcnb.ca/en/news-alerts/cafc-bulletin-cryptocurrency-wallet-fraud)

Canadian Anti-Fraud Centre, posted by the Financial and Consumer Services Commission of New Brunswick (August 2026)

A short government bulletin: what a recovery phrase is, the warning signs of wallet fraud (unexpected contact, "verify your wallet" links, pressure to act fast) and how to protect yourself.

FOR STUDENTS **How To Spot, Avoid, and Report Tech Support Scams** (https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams)

Federal Trade Commission, Consumer Advice

How fake pop-ups, calls and messages pose as tech support, what real companies won't do, and what to do if you already gave access or paid.

FOR TEACHERS **Investigating types of fraud and identity theft** (https://www.consumerfinance.gov/consumer-tools/educator-tools/youth-financial-education/teach/activities/types-fraud-identity-theft/)

Consumer Financial Protection Bureau, youth financial education activities

A free 45-60 minute activity for grades 9-12 in which students match types of fraud and identity theft to scenarios; add a fake "verify your wallet" message as an extra scenario.

Links checked October 2026.

Free to use in class. Educational content only, not financial or investment advice. Episode narration uses a synthetic voice. Answer keys and teacher sheets: email hello@thesteadyblock.com.