CYBER CASH SCAMS

BY JAY BORDEN

Cash is a preferred means of payment for many businesses because it is instantaneous. When someone hands over cash you have it then. No waiting for it to clear or to find that the buyer filed a complaint with their credit card issuer saying they never received the product and want a refund.

Cybercriminals like cash for the same reasons. Once they have it, it is done. Your cash is gone. Cybercriminals don't give refunds.

One of the ways cybercriminals get cash is through scams. Not really surprising. If it was all legitimate, they would be a legal business not cybercriminals.

Let's take a look at some of the methods they use to separate you from your cash.

You receive a call purportedly from a legitimate company. Typically, it's a large company to lend credence to the call and raise the probability that you do business with them. If not, you will be wary about a call from them.

The caller tells you that your account has been compromised by terrorists and is being used to fund their activities. They tell you about some flagged transactions and need you to confirm you didn't make those purchases. There is little chance you did make them as the caller made them up.

You confirm that the transactions weren't yours. Now the caller says that since the activity has been traced to terrorists, the FBI or another federal agency would like to talk to you and have you help them catch the perpetrators.

You agree. The representative from the federal agency joins the call and provides more detail about how your account is being used and to create more fear. They instruct you not to trust anyone and not mention this to anyone including family members.

Copyright 2025. One Brightly Cyber. All rights reserved

CYBER CASH SCAMS

CONTINUED

They say that to protect against your accounts being drained, transfer your money to safe accounts maintained by the federal agency you are speaking to. The money will stay there until the feds shut down the terrorists and their network.

Isn't that a relief, a way to protect your money provided by a reputable agency! It would be, except for one minor detail, the person supposedly from the federal agency is really a cybercriminal. The money you are transferring to be kept safe is going directly to the cybercriminals. Remember what we said above about the attractiveness of cash and that cybercriminals have no refund policy?

Your money is gone.

There are variations on this scam but all involve cash to the perpetrators and the warning to not tell or trust anyone.

In case you think no one would fall for this scam, know that thousands, or possibly tens of thousands, of people are falling for it every day. A cyber researcher spoke to their local bank branch who said they stop 1-3 of these scams a day. With over 100,000 bank and credit union branches nationwide, the number of people being caught by this scam may be enormous.

Some victims go into shock realizing what happened and how much money was lost and require professional help.

This is just one type of scam.

AARP found that 40% of American adults admit to being victims of fraud. Ten years ago, it was 14%. The fraud may involve money, or it could also be private information that was taken, information that is often used to steal identities or commit other crimes.

The Federal Trade Commission had reports of over $12.5 billion stolen through fraud in 2024 but acknowledges the number is probably much higher as many people don't report it.

These are staggering numbers. No one is immune. The victims are people in all walks of life. Even those who think they are too smart to fall for scams.

Copyright 2025. One Brightly Cyber. All rights reserved

CYBER CASH SCAMS

CONTINUED

What to do to stay safer?
Recognize your limitations and that no one is immune. A Nobel prize winning physicist acknowledged losing $2 million to a scam.

Use a unique, complex password for every system or service. Never use the same password for more than one system or service.

Change your password every few months.

Use VPNs, Virtual Private Networks, where possible.

Use MFA, Multi-Factor Authentication, where offered but know it is not fool proof.

Think before acting. If you get a message to change your password, did you request a password change?

If you receive an MFA code to enter, did you attempt to log into the site or application? If not, it is a scam.

Do not download free apps.

Don't take online quizzes. Many are scams to gather information about you or put malware on your device.

Be suspicious, fake messages are getting harder to identify due to the use of AI to generate them.

Knowing what is going on can help you stay safer.

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.

Copyright 2025. One Brightly Cyber. All rights reserved