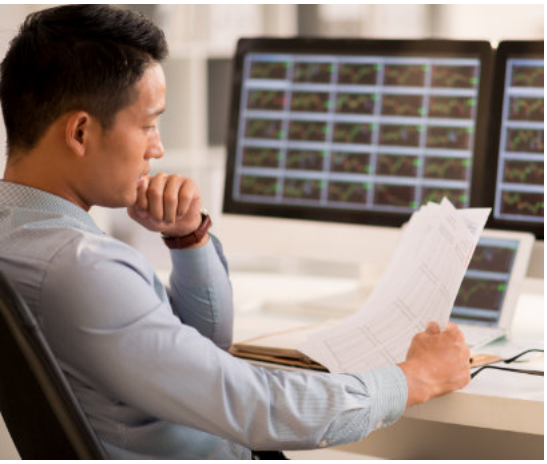
Follow the Paper Trail

Where Does Laundered Money Go?

DEER BROOK



By 2025, cybercrime is expected to result in losses of over $10 trillion worldwide. The United States currently leads in victim and loss totals.

"Cybercrime" is a wide net to cast. The money stolen through cybercrime is gained through a myriad of schemes, attacks, and fraud: ransomware, identity theft, tech support scams, and IRS scams are only the tip of the iceberg.

But what about that $10 trillion figure? Where does all that money go?

Follow the Money

Ransomware, for example, typically demands payment in Bitcoins. On the other end, social scams like romance scams are often exploiting victims into sending over gift cards.

The monetary loss for a victim can range wildly between a few dollars to thousands of dollars. On a particularly bad day, it can escalate into the hundreds of thousands or millions of dollars; these are often the ransom amounts demanded through security and data breaches.

When the criminals get the money, they often attempt to send it through Dark Web money clearing houses as soon as possible. Their goal is to make the money untraceable.

And with a wide berth of tactics and currencies to extort and receive the money in, there's always resources available to turn criminals' ill-gotten funds into real cash.

Money Laundromat

The typical money laundering cycle kicks off with a handoff. The stolen cash is forwarded to an intermediary who has the skills and resources to launder the funds through offshore shell companies or digital clearing houses.

After a fee is deducted, the intermediary sends the laundered funds back to the original criminals who stole it.

Transnational organized crime is increasing on all cybercrime fronts. Cybercriminals' networks are rapidly increasing their involvement in cybercrime itself, which is costing U.S. consumers billions of dollars in losses.

Bit by Bit

It might be emotionally devastating, a $50 item that's never delivered isn't often financially devastating. But from the scammer's perspective, that $50 coupled with the $50 of a thousand other victims quickly adds up into serious money; it all adds up, and even the smallest losses matter.

Where Does It Go?

Stolen money often ends up funneling through and supporting varied criminal or terrorist organizations all around the world.

One source close to Deer Brook reported that they tracked $93 million stolen in the U.S. to Russian money exchange akin to PayPal. Later, this money was found again, forwarded to a terrorist organization in the Middle East.

Being Proactive

We can all play a role in cutting off the cybercrime funding flow by protecting ourselves from cybercrime and scams. Practicing general cybersecurity awareness, regularly reviewing accounts, and scrutinizing payments from all your accounts are a great way to start.

Passwords

Never share your password, and don't use iterations of the same password across your accounts. For example, if your main password was "password1," don't use iterations like "password2" or "password3."

Don't save passwords in your browser. Use a password keeper program or keep hints for yourself elsewhere.

Gift Cards

If you receive an unexpected email that asks you to log in or click a link, either discard the message or contact the sender directly (and not via email) to verify its legitimacy. Never respond to emails that refer to or ask for gift cards.

And before buying gift cards, check the packaging for tampering; criminals have been known to open gift card packaging, steal the code, and wait until the card is charged to then grab the money.

Finances
Use multifactor authentication; using an authenticator app as opposed to SMS is the strongest possible option. Legit apps and systems that handle finances will always have MFA as an option.

Report scams related to your banking account to your bank or credit union as soon as possible. Any scams resulting in a loss can be reported to the FBI on their website, IC3.gov.

If you get a phone call related to your banking account, or any online accounts, ask for a case number or a ticket number. Hang up and call them back on a phone number you know is valid.

In addition, the IRS will never send emails about your accounts, taxes, or penalties. They exclusively use the United States Postal Service.

General Upkeeping
Don't browse risky websites, and don't respond to tech support alerts in your web browser. These are one hundred percent fake.

Keep your computer, tablet, and mobile devices updated. It's also just as important to make sure your software on these devices is updated as well.