GlobalResearch
Center for Research on Globalization

Cyber Risks, the Achilles' Heel of Cashless Economies

By William Davis
Global Research, September 05, 2018

Region: Europe, USA
Theme: Global Economy

Note to readers: please click the share buttons above

Newspapers around the globe are telling us that contactless payments are thriving, cash is rapidly disappearing and cashless society is practically around the corner.

You don't need cash to pay for your groceries anymore, and don't be afraid if you forgot to take your wallet with you – just use your smartphone. Carl Scheible, Managing Director of PayPal UK, summarizes [1] the current situation:

> "We'll see a huge change over the next few years in the way we shop and pay for things … you'll be able to leave your wallet at home and use your mobile as the 21st century digital wallet."

Some are dissatisfied with this state of affairs. In this case, the classical tactic of intimidation becomes the main argument of champions of cashless society. Cash is used by criminals; our children can buy drugs with cash; cash supports the shadow economy and encourages tax evasion – these are just some of these loud statements.

Ability to present control as protection is based on constant calls to think about an external enemy, that is terrorists or mafia. This element of moral panic is contrasted with friendly and unobtrusive advertising of digital payments. The newborn cashless society is emerging like the sunrise, washing away these dangerous dirty banknotes with the rays of hygienic and convenient digital salvation.

This rosy picture is completed by speeches of academicians, economists and futurists that live in green suburbs, fly business class and demonize bills and coins.

> "Without cash, we would live in a much safer, less violent world with enhanced social cohesion, since the major incentive fueling all illegal activity [i.e. cash]… would disappear," believes [2] Guillermo de la Dehesa, a Spanish economist and current international advisor to Banco Santander and Goldman Sachs.

And the trick is working. Cash is being excluded from the official economy, and tellers are watching with suspicion while you are fumbling for coins in your wallet. There is a sign on every other store: *"No cash accepted*".

However, the same system that facilitates the unhampered flow of information and its use for commercial purposes, also provides technically dexterous criminals with almost limitless

opportunities to capitalize on their neighbor. How is it possible? Let's see.

Why it's wise to be a little bit paranoid

It won't take long to figure out why we have become vulnerable to cyber crooks:

- In 2017, 2.73 billion people worldwide will use [3] a mobile phone to connect to the internet
- Among people under the age of 24, four in ten internet users were using [4] online banking, while over one in two internet users between the age of 65 and 74 were engaging in internet banking across the EU in 2016.
- Nearly two thirds of internet users in the European Union made [5] online purchases in 2015.

The online world is penetrating into all aspects of our everyday life, from paying taxes to hiring and changing the mailing address. And as commerce is turning digital, we are becoming increasingly defenseless against intruders. Steve Morgan, the founder and CEO at Cybersecurity Ventures, published [6] some figures regarding the issue:

- Cybercrime damage costs will hit $6 trillion annually by 2021
- About 6 billion people will become victims of cyber-attacks by 2022
- Global ransomware damage costs are predicted to exceed $5 billion in 2017

These are impressive figures – which is not surprising, because it's profitable to be a cybercriminal. Trustwave claims spammers can earn [7] up to 90,000 euros a month. Price for various malicious software starts from 120 euros while the profit can grow ten times bigger.

It doesn't get any easier with the fact that cybercriminals are incredibly difficult to catch. The world industry of cyber security is still not completely sure who stole the money from the bank of Bangladesh – and it's been more than a year since then!

Leo Taddeo, a former New York FBI special agent in charge of fighting cybercrime, explains [8]:

> "Hackers use tools to disguise their IP address. Other technologies like Tor and encryption add other layers to make it difficult to identify them. These tools are widely available. They make it a resource-intensive and time-consuming task to find hackers."

Worst of all, users remain unprotected, being subject to risks of theft. Fair and square, the bank should be held responsible regardless of guilt, since it carries out risk-based activities. However, this rarely happens in reality – the only exception is that the money will be returned in full when the creditor's fault is proven. Yet, it is incredibly difficult to prove the guilt, because banks always provide themselves with a backdoor for cases like that. Simply put, nothing depends on you with non-cash payments, and there's no adequate protection.

To be the sole owner of your money

Is it possible to avoid these risks? Perhaps it's worth going back a bit and regaining responsibility for your own money – with help of cash.

Keeping a part of money in cash as a war chest allows us to rely on ourselves. If there is no public confidence in non-cash settlements, then no measures, even punitive ones, will help.

Partly for this reason, cash payments are still very popular. We need cash not only because of the lack of necessary infrastructure and logistics in remote geographic areas, but also due to growing crises in the politics and economy of many countries, distrust of banking and payment systems, cyber risks of cyber-attacks and cyber-fraud. Despite the ecstatic claims that cash is dead, the demand for cash is still climbing up [9] across the United States and Europe.

After all, if the cash is really "dying", then why does its share in money turnover is growing, and why investments in improving cash circulation are so large? No one would waste huge sums on initially unpromising projects.

Source: techjury

*

William Davis is a PhD student in Economics.

Notes

1. www.cgap.org/blog/allure-cashless-society
2. wolfstreet.com/2015/04/25/don-quijones-war-on-cash-quotes-to-cashless-society/
3. www.emarketer.com/content/emarketer-updates-worldwide-internet-and-mobile-user-figures
4. www.independent.ie/business/irish-above-eu-average-for-online-banking-but-lowest-for-news-35991299.html
5. ecommercenews.eu/65-internet-users-eu-shopped-online-2015/
6. www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
7. www.sentryo.net/the-new-professional-cybercrime-industry-ever-more-lucrative-and-threatening/
8. www.raconteur.net/technology/catching-hackers-is-not-getting-easier
9. www.cashrepository.com/2017/03/myth-cash-demand-is-declining/

Articles by: William Davis