It does not always have to be Panama

Not only the mailbox paradise in the Caribbean, but also the daily used Internet is considered a new focal point for money launderers. Criminals use dirty tricks to net blue-eyed users for their machinations.

Only film stars or investment bankers no matter about lthousands of euros a month. Especially when the considerable sums are to flutter almost without effort into the house. Such a message from paradise could only be found by e-mail addresses in their mailboxes. As sender named “Springinklee Services", a “well-positioned" company looking for staff “who appreciate good money for effortless work”.
The casual activity was by no means the folding of prospectuses in homework or telephone jamming of used car buyers. But a job that will never appear in a job ad. The work did look too simple at first sight to be true: for if the prospective buyer were to want that generous wage, he simply needed to make his account available. Afterwards, the company completed transactions abroad. What all the new employees who were to receive a 20 per cent commission from each of these transfers were later registered: they were abused as "financial agents" or less flattering than "Money Mules" (Geldesel) and got no tired cents from the new employer who had sent a serious working contract. The money transferred was from, among other things, offenses such as illegal arms, drugs or human trafficking. In such pseudo-entrepreneurs, who are fishing with super salaries blue-eyed citizens, are criminals, who want to create hot financial returns from the field of vision. Quick, unobtrusive and well camouflaged. What is sold as a pleasant sub-job about refined recruiting mails has in practice an unpleasant name: money laundering.
For this „cleaning” today it is enough to have a computer as a modern escape route, a as unlit as possible driveway to the data highway as well as enough dirty tricks. The possibilities of the digital era have not been hidden from the organized crime. So the network mutates into the point of contact for financial offenses, which no lawmaker should ever notice.
"As the economic life is increasingly shifting to the Internet and this development is progressing rapidly, an ever increasing use by criminals is to be expected.
The attraction points for such persons are the anonymity and speed with which global transactions can be concluded, "explains Rudolf Unterköfler, head of the Department of Economic Criminality at the Federal Ministry of the Interior.
After all, it is about huge sums. All in all, the amount of gobal money laundering should reach a volume of one to two trillion dollars a year, as the currency transport is worthwhile via digital paths. "For criminals, it is immensely important to conceal the origin of illegal revenues. In the Internet nobody asks for the origin of the money, no one redirects suspicious messages. In this network, which allows global actions, the imagination knows hardly any limits", says Heike Samel, expert of the company consulting Sopera Steria Consulting.
Another evil deception maneuver confirms this new trend of gel cosmetics, which is intended for users to take part in: Here the disaster starts again with tempting job adverts, this time placed on lesser known online small advertisement portals. In the offer are logistics jobs, over average highly endowed, timely flexible and of course without effort to cope. Who will say "Yes" to this dream job, the service contract is send to enter the address, account number, cell phone number and availability during the day and return the document.
A “staff member” of the company will provide telephone instructions for the work area. The new colleague should repackage goods delivered to his home and send them to foreign recipients. With

his sender. The motivated newcomer is already working as a „package agent" and makes computers, smartphones or Prada fashion ready for travel. Desperate attempts to contact the supposed colleague after teh missing salary remain unsuccessful: All email accounts are deleted, telephone numbers no longer work.

After all, the wire-pullers behind the dubious mail-order business have done their job and have long since gone all over the mountains. With very good reason: the shipped, usually high-quality products were bought in online shops with previously stolen credit cards. The criminals can´t happening anything: Gangster remains in the dark, useful traces are shortageware - except for one, the one to the part-time logistician. It is possible that no detectives are ever ringing. But coincidence should strike a chance or a little well-to-do neighbor, who is suspicious of the multitude of packages, calls the number of the police, it can be bitter. "Thus, an innocent citizen turn in someone who has made himself a criminal.", warns Samel. "In case of suspicion, this person, the smallest member in the chain, saves the investigators on the silver tray and often remains the only one who is then held responsible. A financial penalty or worst possible detention ist to be expected."

Ignorance can not be regarded as an excuse. Where basically anyone can fall into the trap, which quickly needs bares and put his brain off. To this constellation hope attackers. „Faithful believers, who see their chance for quick money, become middle-class men. Money launderers like to give up on private ones, since they do not have to legitimize themselves here. In principle, everyone who has an account can become a victim", says the stepping-up message from Dieter Steiner, head of the security service provider SSP Europe. Certain groups are paying particular attention to the dark side of the web: retirees, the unemployed or the socially weak for understandable reasons as easy prey. On online dating portals, lonely people can be found, who are prone to hollow promises of the huge remuneration for zero effort, the gangsters behind the monitors have tried to trust. However, insiders are also afraid that soon a new group will spark the interest of unscrupulous money launderers: refugees who are familiar with digital life, have an account, and are struggling for every kind of straw because of their difficult economic and social situation. Even if reason should say something could stink here.

It is by no means easy for third parties to recognize threatening judgment immediatley. Behind the online ordering of holiday doses, only parapsychologically trained TV cops would see a risk, but this exists. At the beginning is still everything normal for the landlord, the deposit of the guest as confirmation of the booking is coming in. After a short time, the paper turns radically: the lyre-no-traveler informs with regret that he has to stay at home and therefore asks for a quick refund of his monetary advance.

That would not be unusual. But at the same time, the amount should no longer be transferred to the original account. A bank connection abroad acts almost as if out of the blue as a new monetary runway. Landlords, who are not well with the matter, are covered with flimsy explanations and put under pressure. Who finally gives in, has already made his fingers dirty, because the holiday payment comes naturally from dark sources.

However, Steiner, who points to simple home remedies as prophylaxis, said that this kind of treatment is by no means an inescapable destiny: "Frequently the healthy understanding of the people helps. All-too-tempting offers for extra earnings or e-mails with the demand to disclose delicate personal data should be considered critically. Regular checks on account statements can´t be detrimental." This penile control may save a nasty surprise. Because sometimes the money laundering procedure runs completely discreetly in the background. The code word is phishing: The generic term, consisting of password and fishing, means a largely silent online attack to harmless consumers: the theft of personal financial data runs through fake e-mails, the official notifications of the credit card company or the house bank are almost deceptively similar. Anyone who reacts to electro post in spite of years of warnings,

asking the trusted credit institution to click on the included link and enter its account number because of a security check, has already lost. These data end up with the senders of the e-mails, which clean dirty money over that stolen bank connection. Should the lawful owner only view his bank statements at Easter and New Year, fraudsters have easy play.
Criminals are hoping for a new tool that will make the money clean up even more effective. These are digital currencies which, according to experts, should play a special role. The most common variant is named "Bitcoin", a linguistic combination of bit, the smallest memory unit in the computer, and Coin, English for coin. It is a payment means that exists only around the Internet, has not been controlled by any bank and is available on special Bitcoin exchanges against real cash. While serious industry professionals are still discussing the purpose and the future of such financial alternatives, gangsters have long ago ordered the value that is relevant to them. Almost 100 per cent anonymity turns the online purchase of valuable goods with converted black money into a children's game as well as the return of the e-moneys into analog notes. Kristof Wabl, a specialist in consulting firm PwC Austria, says: "Virtual currencies have no physical existence but only leave behind digital traces, and the origins of these sums are disguised by complex financial transactions. The money lured here is then transferred to an anonymous account, fixed on a money machine and this track disappears. "

The original article can be found at https://www.ssp-europe.eu/fileadmin/Content/PDF/2016-04-23_-_Profil_-_Internet-Geldwaesche.pdf.