
Remote access and
social engineering risks
prevention best practices

TABLE OF CONTENTS

1. *What is a remote access technology?.....3*

2. Remote access: application scenarios & risks.....4

3. Social engineering: how it works?.....6

4. Main types of attacks.....7

5. How remote access can be spotted?.....8

6. Protect your company: short checklist.....11

1. What is a remote access technology?

Remote access technology refers to any set of IT tools used to connect, access or manage devices, resources and data stored on a local network from a remote geographic location. You may ask, so how this is different from using a cloud solution? The thing is that remote access technologies provide access to an on-premises environment rather than being hosted out of the office in a shared environment and they are accessible via the Internet. Three most common remote access technologies are Remote Desktop Services, remote access software and VPNs.

We can't but agree, remote access remains a very important tool for those companies, which have not yet migrated to the cloud or need access to on-premise computers or resources. With this access users can manage files and data stored on a remote device, it also allows them to continue to collaborate and keep a productive work from any place in the world.

2. Remote access: application scenarios & risks

Remote access technologies are very popular in the IT industry. The scenario of remote access application is quite extensive:

- Testing programs;
- Storing files in the cloud and granting users access to it;
- Solving technical issues
- Remote work setup (for ex.: virtual private networks).

However over the past few years financial institutions have seen how these technologies may do harm to both - lenders and potential borrowers: the increased growth rate of online fraud is caused not only by technologically advanced fraudsters improving their tools, but also by expansion of remote access technologies use by a wide range of individuals, including technically advanced ones and much less tech-savvy.

Today we will talk about the best methods, which will help online businesses to deal with the problem of social engineering and remote access and also will shed some light on the issue of **protection from these types of risk.**

There is one glaring problem with remote access technologies in credit risks: they can be used by fraudsters to log in to a personal account in order to read SMS with a passcode or apply for a loan on user's behalf. In addition to that, there is an abundance of additional social problems: fraudsters usually attack socially unprotected population, for example, aged people.

Financial institutions constantly develop online channels for financial services rendering, expand the range of products and services, make their products more accessible to different categories of customers and also solve many social and economic problems associated with financial inclusion.

Being aware of this, fraudsters, in turn, improve their tools, use a combination of social engineering and remote access technologies to attack such categories of customers. Consequently, these types of attacks are often effective, so making financial institutions aware of the remote access tools on the borrower's device makes it possible to counteract such situations and reduce the number of such fraud cases.

The statistics of successful attacks performed by means of remote access and social engineering is shocking: according to our data, when a fraudster draws up a loan agreement with the withdrawal of funds to a debit card, the client gives away 2-3+ SMS or one time password codes on average.

3. Social engineering: how it works?

Social engineering is a fairly broad term that refers to a type of fraud when criminals influence a person through psychological manipulation in order to directly steal money or in order to obtain sensitive and personal data (for example, passport data, login and password from an online personal bank account) for the subsequent commission of a crime and theft of money. The main channels are social media and phone calls.

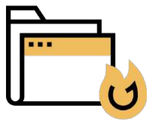
According to JuicyScore, **60-70% of professional social engineering scams follow this pattern**:

A user receives a call from an unknown person, who pretends to be an employee of a bank or any governmental authority. In some cases, number spoofing, call center imitation and IVR can be used. After that a scammer fraudulently lures the data, reporting false information, for example, that passwords and accounts are at risk and requests user's personal data: card details or an SMS code. Also he usually offers to download “official” bank application in order to protect user's funds. Such application is often nothing but a remote access program. On collecting victim's personal data, scammers enter personal account using remote access technologies and make a purchase, card2card transfer or apply for a loan on user's behalf.

4. Main types of attacks related to remote access and social engineering fraud

There are several types of attacks associated with the use of remote access technologies. According to our data, the first two types are the most common:

Use of special malicious plug-ins or "prepared" browsers;



An attack made by infected computers (most often through virus mailings, containing malicious links with dangerous programs and applications);

Passive social engineering - when a person gives away some information during a call or installs special applications, while fraudsters do the rest;

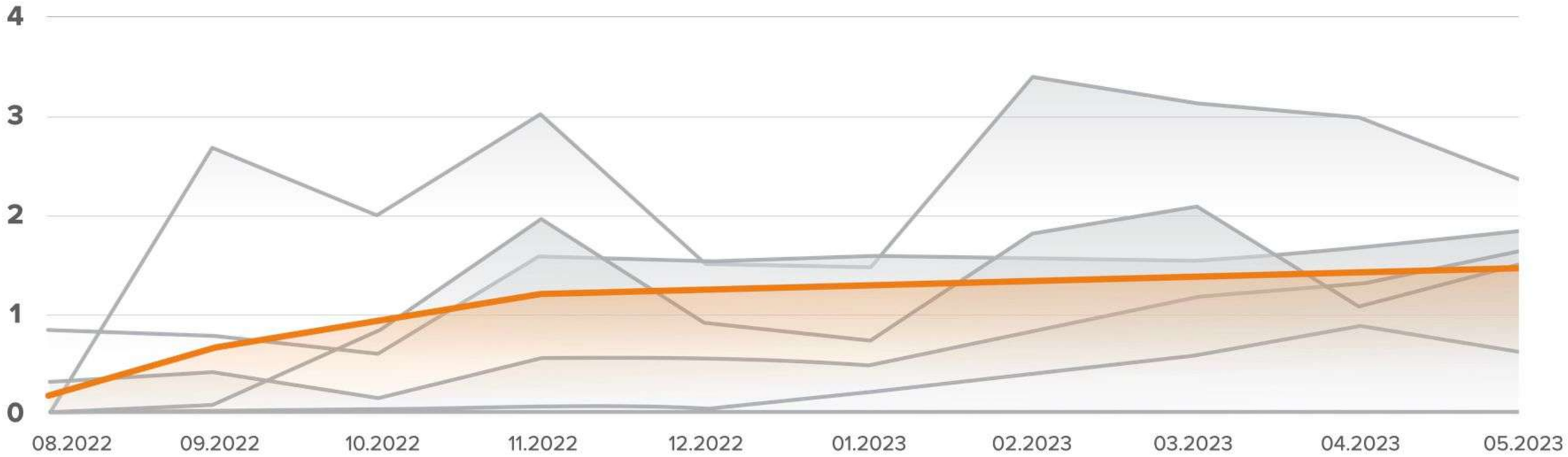
Active social engineering - when a person does everything with ones own hands (including the last transfer of funds or applying for a loan), and the attackers only tell the victim what to do (often they are in the office or somewhere not very far the person - they tell the victim to install malware, download the application from a link, say password from SMS and so on). This is the most difficult case to spot and to investigate as well.

5. How remote access can be spotted?

JuicyScore

Number of applications in the flow with signs of remote access by region, %

Regions: EU, Eastern Europe, Africa, South Asia, APAC, Latin America.



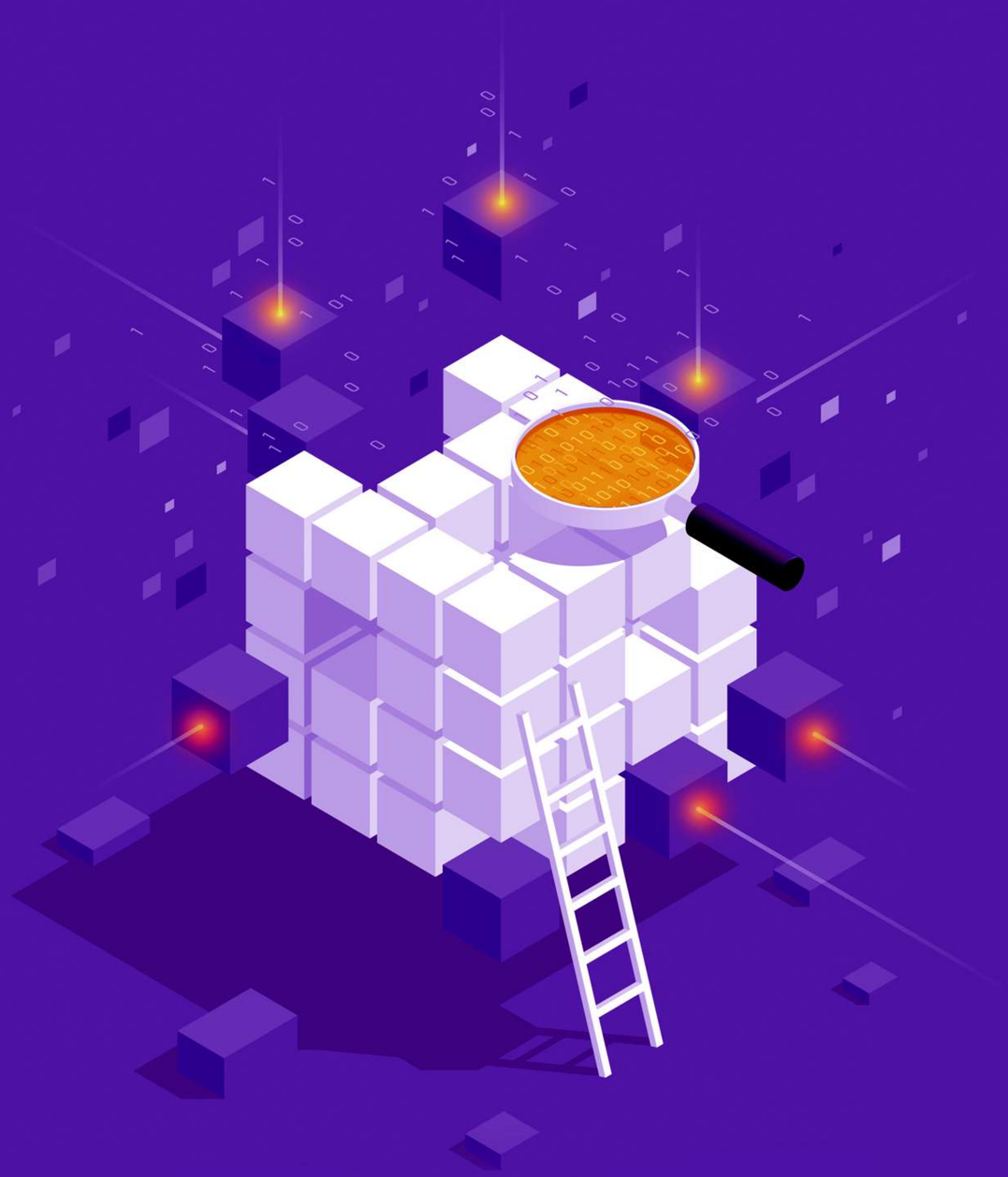
5. How remote access can be spotted?

As you may already know, the best way to protect personal data is not to use it. JuicyScore team is able to determine the presence of remote access technologies during the session, to be precise, directly at the very moment of filling in an application for a financial service or product obtaining.

We tracked the dynamics of devices with signs of remote access we spotted recently and came to the conclusion that this indicator tends to grow.

We developed a few ways, which proved to be the best in spotting remote access technologies. They also can be effective in remote access fraudulent applications detection.

We collect as much information as possible that a browser can legally give out through different browser APIs, after that we analyze such data and identify typical signs of virtual machines or malicious plugins presence. And we are eager to show our short check list how to protect your company from remote access and social engineering fraud.



JuicyScore

Protect your company:

Short checklist

6. Protect your company: short checklist

Here are some of the features which are absolutely necessary in order to spot remote access and social engineering:

- Dangerous plug-ins and randomizers specific to remote access spotting;
- Active dangerous applications and remote access applications on the device spotting;
- Injections during online sessions spotting;
- Specific anomalies in the traffic characteristics of the device and its connection spotting;
- Device parallel activity presence spotting.

We are constantly discovering new tools for detecting social engineering technologies. Based on our data, we can say that the number of sessions with signs of remote access is about **2.5-3%** of the total flow of applications. This fact may serve as a signal for online lenders that it is high time to pay attention to such applications and introduce additional verification. Book a demo with us to learn more about fraud detection and prevention techniques in your region.

Contact us now: https://juicyscore.ai/en/ready-to-connect/

JuicyScore

PROTECT YOUR BUSINESS

and let it grow without risk

info@juicyscore.com