POLITIE

# Tech Support Scam: ‘disconnect’

Report regarding the end date of the Declaration of Intent to Disrupt Tech Support Scam.

Project team Tech Support Scam

Final

« waakzaam en dienstbaar »

# Table of contents

# Foreword

You have before you the final report of the project ‘Disruption of Tech Support Scam in the Netherlands’. A project that started with the observation that this was the form of cybercrime that was most often reported at the time. Extra worrisome, because in 2016 and 2017 the number of Dutch victims grew rapidly. Now, at the end of 2020, we can conclude that the growth in the number of victims has been brought to a halt and that the damage per victim has decreased considerably.

This project shows that a coalition of government bodies and national and international private parties can lead to effective national prevention campaigns and the putting up of barriers. This makes it more difficult for criminals to make victims. Because each party, from a common goal and with respect for everyone's position, does everything possible to achieve that goal.

We are proud that this has been achieved on the initiative of the police and the Public Prosecution Service. An initiative in the best Rotterdam tradition of 'don't bullshit, just do it'.

One last appeal to all potential victims: hang up! Disconnect!

Hugo Hillenaar
Chief Public Prosecutor

Fred Westerbeke
Chief of Police Rotterdam Unit

# Introduction

In 2017, it was established that the number of police registrations on Tech Support Scam increased significantly to almost 2000 registrations in that year. This turned out to be one of the forms of cybercrime that was most frequently reported in the Netherlands in 2017, with an estimated loss of almost EUR 6 million in that year. The police and Public Prosecution Service have taken the initiative to approach several parties in order to stop this.

Although various types of companies can become victims of this crime, in the sense that their name, service or product is abused by fraudsters, a start has been made in the Netherlands to approach parties most often mentioned by Dutch victims. Because Tech Support Scam is internationally organised, these were also parties that were organised internationally.

This has resulted in a unique public-private collaboration. This collaboration was confirmed by the signing of the 'Declaration of Intent of the Broad Coalition for the disruption of Tech Support Scam in the Netherlands' on 28 March 2018. The parties involved in this were:

1. The Minister of Justice and Security
2. Public Prosecution Service
3. National Police
4. Netherlands Authority for Consumers & Markets
5. Microsoft Corporation
6. TeamViewer GmbH
7. Koninklijke KPN N.V.
8. VodafoneZiggo Group Holding B.V.
9. Western Union Company
10. MoneyGram International Inc.
11. ABN AMRO Bank N.V.
12. ING Bank NV.
13. Coöperatieve Rabobank U.A. (Rabobank)
14. Volksbank
15. Verenigde Bitcoinbedrijven Nederland (VBNL)

Later on, the Dutch Payments Association became involved.

Over the past period, investments have been made to establish good cooperation, to build the network and, of course, to implement measures to disrupt Tech Support Scam where possible.

The Declaration of Intent ends on 31 December 2020. With this report we give you a brief insight into the developments about the phenomenon, the cooperation and what the results have been of the joint efforts.

# The phenomenon

- We speak of a Tech Support Scam if there has been telephone contact between the fraudster (who acts as a solver of technical problems with the computer) and the victim. Usually, after installation of a Remote Access Tool, money is transferred without the consent of the victim. Social engineering plays an important role.
- The main features of the forms of Tech Support Scam have hardly changed in recent years and mainly consist of: being called', 'helpdesk search' and 'pop-up messages'. This form of fraud still mostly takes place in the English language.
- It is complicated to make criminal investigations successful because the telecommunications, digital and financial traces, if they can be traced, always lead abroad (and even sometimes to different foreign countries on a case-by-case basis). What is more, these traces are fleeting and cooperation with non-European countries is not always rapid.

**Explanation of the phenomenon**

In November 2018, an in-depth analysis[1] was drawn up for Tech Support Scam or helpdesk fraud or Microsoft fraud. This provides a clear picture of this phenomenon. This information was updated in 2020.

Tech Support Scam is a form of fraud in which telephone contact takes place between the target (the victim) and a person posing as an employee of a software company, for example Microsoft (the fraudster)[2] . As a result of unauthorised access to a victim's computer, the completed crime usually falls under cybercrime in a narrow sense (crime with ICT as a means and a target).

The reason why this fraud was originally called 'Microsoft scam' is because this name is most commonly used in the fraud. This is related to the fact that victims also make extensive use of this software. It is therefore credible for victims if someone pretends to be a Microsoft helpdesk employee. The information shows that this is still the case to this day.

Within the modus operandi, 'social engineering' is applied, whereby attempts are made to gain access to systems and confidential data of persons through deception and persuasion and to have them actively participate in the fraud. The fraudsters mislead victims by pretending to be a trusted party, i.e. a helpdesk employee, technician or security expert. In addition, the fraudsters use social influence (a change in a person's attitude, beliefs and behaviour as a result of internal or external pressure), using various persuasion techniques distinguished within psychology. The ultimate goal of the fraudster is to make the victim pay money for the so-called service provided and/or the misuse of personal data of the victim that are on the computer, in order to make transfers at the expense of the victim.

More people are active online and digital remote assistance is becoming more and more common. In addition, more and more data is stored digitally, which makes the need for a secure environment crucial. Tech Support Scam will therefore be inevitable in an increasingly digitised society.

### Definition Tech Support Scam

When signing the Declaration of Intent, the following definition of Tech Support Scam was included:

- A number of types of fraudulent activities by telephone, in which a fraudster claims to offer legitimate technical support services. The calls are made via cold calling to unsuspecting users, or take the form of enticing users to call a particular phone number, for example through a browser pop-up.
- In the Netherlands, this fraud usually targets Microsoft or Apple users, with the caller often claiming to represent the technical support service of these companies when this is not the case.
- In typical cases, the fraudster will try to get the victim to give access to his computer remotely. Once remote access has been obtained, the fraudster attempts to gain the victim's trust in order to pay for so-called support or other cunning tricks are used.
- Subsequently, the victim is prompted to transfer an amount of money to the fraudsters, for example via a bank transfer, money transfer, gift cards, etc.

[1] In-depth analysis TSS dated 30-11-2018, Jildau Borwell and Kirsten Bos-Riepma

[2] Broad coalition to disrupt Tech Support Scams in the Netherlands, 2018.

**Modus Operandi (MO)**

*1. The victim is called on a fixed or mobile telephone number (manifestation: 'being called').*

The victim is called on his fixed or (nowadays more common) mobile phone number, after which the English-speaking caller introduces himself as an employee of Microsoft or another software company. This is also known as 'cold calling'.

*2. The victim searches online for help with computer problems (manifestation: 'online help search')*

The victim searches online, using a search engine, for help with computer problems. The fraudsters have set up convincing websites that come across as help desks for various software companies such as Microsoft, McAfee, Avast and Skype. These websites appear high up in the victim's search results. When the victim calls the telephone number of the 'helpdesk' in the search results, they get a fraudster on the phone pretending to be an employee of the company in question.

*3. A pop-up appears in the victim's screen (manifestation: 'pop-up')*

Victims are shown a pop-up screen on their computer, often accompanied by alarming sounds or flashes, that they cannot (easily) click away and is often image-filling (Harteveld & Bloem, 2018). The pop-up states that the computer has been infected with a virus, the files on the computer have been encrypted or child pornography has been found on the computer. The victims are asked to call a (often Dutch-looking) telephone number.

*After the above-mentioned variants, the way in which the persons are cheated out of their money is often the same:*

After the victim is convinced that the 'solution' of the technical support has to be paid for, the price that should be paid for this is discussed and the victim logs on to the internet banking environment. By using the Remote Access Tool, the fraudster has the possibility to set up a 'black screen' or greatly reduce the size of the screen. After logging on to the online banking environment, the fraudster has the possibility to adjust the displayed amounts and thus falsify the screen. When the screen is normalised again, the victim is misled about the beneficiary and the amount to be transferred. The money is transferred to bank accounts abroad or cryptocurrency (e.g. bitcoins) is bought with it.

Another common way is to pay with gift cards (pre-paid cards, I-tunes, etc.). The victims buy these cards and then pass on the code.

*Geographic decisive factor*

It is generally known that Tech Support Scam has its origins in India and to this day it is still very likely that many operations are carried out from this country. The reasons for this may be:

- The history of India as a colony of England as a result of which the English language prevailed and is still spoken today.
- India was one of the first countries to outsource, partly because English was spoken and because of its low costs. As a result, networks are available for, among other things, communication with the source country.
- India has grown into an IT superpower with all kinds of renowned training institutes[3] in this field. The relatively high level of education in combination with high unemployment makes it easier to choose to participate.

The above cannot be confirmed 100% from the police information because it is difficult for the injured party to name the English-speaking and specific accent. However, digital and financial traces of a number of Dutch police investigations do indeed appear to originate in India.

In addition, on the basis of information from the domains and associated email addresses from 2020, it appeared that approximately half of the fraudulent domains investigated were registered in India. Of the other half, it is not traceable in which country they were registered because they shielded this information. Although just registering a domain name does not directly imply that the fraud would also take place from India, this is also an indicator that this is the case.

Previous requests for cooperation with India on this phenomenon have so far proved unsuccessful. As a result, this report also lacks insight into criminal networks and it is not always possible to answer underlying questions such as about the revenue model (per sub-MO) or how the data is obtained to approach potential victims.

[3] https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

## Collaboration and measures

By looking at the Tech Support Scam from the point of view of each partner together, various disruption measures could be taken. Cooperation was the key word.

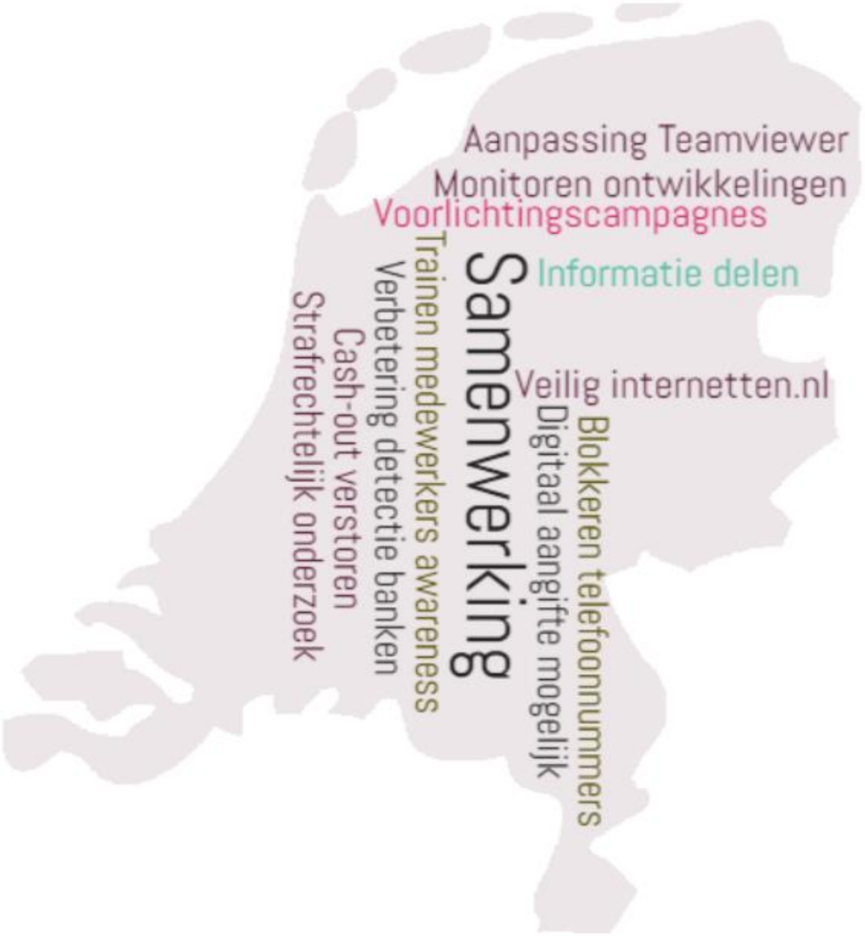
### Cooperation process

The main common ground was that the parties recognised that the incessant attacks by Tech Support Scam do not only threaten public confidence, but can also damage the reputation of the various private parties.

After the signing of the Declaration of Intent, consultations with the partners took place once every three months under the shared chairmanship of the Public Prosecution Service and the Police. These used to be physical meetings, but since COVID-19 this has been organised digitally. The police drew up a quarterly integrated security picture. This was based on data from the police and the data supplied by the other parties. This made it clear whether there were any changes in the manifestations, the development of loss amounts, etc. The meetings included a discussion on the basis of the aforementioned security picture about which disruption measures could be useful to reduce the number of Tech Support Scam victims and/or limit the damage. Based on this, various parties took the initiative to implement suggestions made.

### Disruption measures

Although not only in the Netherlands, but all over the world, many people fall victim to Tech Support Scam and global measures are desirable, it has been agreed in the context of feasibility to start with measures at national level. Below is an overview of a large number of these measures:



A number of these interventions are explained in more detail:

## Cooperation

One of the most important successes has been the creation of a broad network. This unique cooperation has been the basis for tackling other similar phenomena in cybercrime as a whole. The fact that the network is already in place makes it possible to consult each other more quickly about possible barriers and interventions.

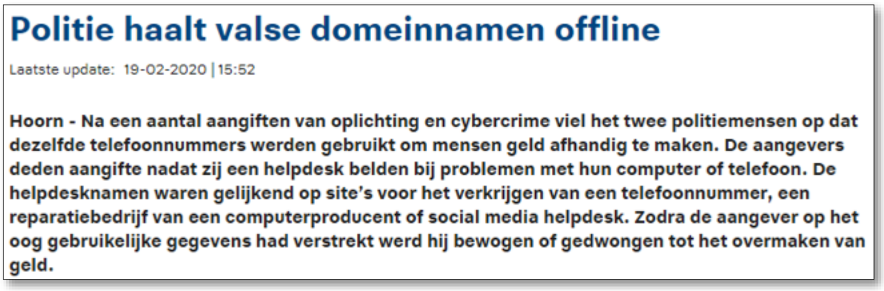
## TeamViewer

Based on the original data, it appeared that especially TeamViewer was used as a Remote Access Tool for Tech Support Scam. After sharing this information, TeamViewer adapted the software where possible to prevent misuse. After this modification, it appeared that the use of TeamViewer for Tech Support Scam has decreased significantly. In addition, TeamViewer also has a site (https://www.teamviewer.com/en/report-a-scam) where users can report fraudulent use of this tool.

Unfortunately, it has also emerged that the fraudsters subsequently use other parties that offer Remote Access Tools where there is no threshold (yet) to prevent abuse as much as possible. The coalition has also contacted these parties and brought them into contact with TeamViewer to share this successful approach.

## Police

In addition to criminal investigations into the offenders, efforts have also been made to bring down fraudulent helpdesk websites. A number of official reports showed that victims had called a telephone number that they had looked up on the Internet, but which in retrospect was fraudulent. A well-known example of this is klantenservicenederland.nl. By order of the Public Prosecutor, this website was made inaccessible in November 2018. The perpetrator evidence also leads abroad from this website. Unfortunately, making a website inaccessible is only a temporary possibility; in addition, similar websites soon appeared operational again.



**Politie haalt valse domeinnamen offline**

Laatste update: 19-02-2020 | 15:52

**Hoorn - Na een aantal aangiften van oplichting en cybercrime viel het twee politiemensen op dat dezelfde telefoonnummers werden gebruikt om mensen geld afhandig te maken. De aangevers deden aangifte nadat zij een helpdesk belden bij problemen met hun computer of telefoon. De helpdesknamen waren gelijkend op site's voor het verkrijgen van een telefoonnummer, een reparatiebedrijf van een computerproducent of social media helpdesk. Zodra de aangever op het oog gebruikelijke gegevens had verstrekt werd hij bewogen of gedwongen tot het overmaken van geld.**

[**Police take fake domain names offline**

Hoorn - After a number of reports of scams and cybercrime, two police officers noticed that the same telephone numbers were used to cheat people out of money. The persons reporting reported this after they called a helpdesk for computer or telephone problems. The helpdesk names resembled those of sites for obtaining a telephone number, a repair company of a computer manufacturer or social media helpdesk. As soon as the person making the report provided apparently usual information, he was moved or forced to transfer money.]

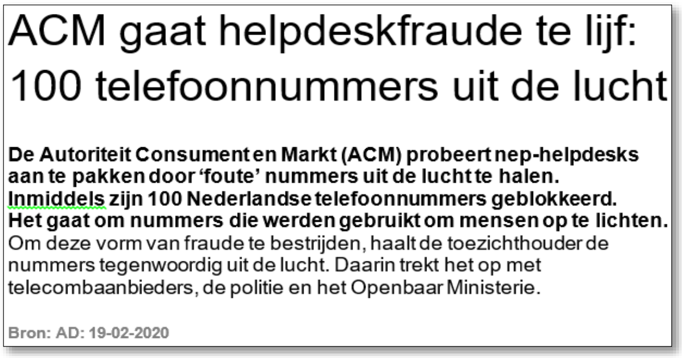
In addition, the police have made it easier for the public to report digitally. The unambiguous and extensive questioning has created a good insight into this fraud and this offered, among other things, added value for the provision of information to the partners.

## Adjustment customer identification process Verenigde Bitcoinbedrijven Nederland (VBNL)

The affiliated companies affiliated with VBNL have adjusted their due diligence on the basis of the information. This made the criminal cash-out more difficult and also ensured that the amounts of the losses (compensation) for the bitcoin companies decreased considerably. They also invested in training staff to be able to identify fraudulent acts in good time. What has not yet been realised, but is still on the agenda, is not only national, but also international cooperation with bitcoin companies.

## ACM: Blocking telephone numbers

On the basis of the official reports, the police periodically shared fraudulently used telephone numbers with the Netherlands Authority for Consumers & Markets. If, after careful investigation, it appeared that the telephone number was used for Tech Support Scam, the ACM, in cooperation with the telecom providers, ensured that the number was blocked.



ACM gaat helpdeskfraude te lijf: 100 telefoonnummers uit de lucht

**De Autoriteit Consument en Markt (ACM) probeert nep-helpdesks aan te pakken door 'foute' nummers uit de lucht te halen. Inmiddels zijn 100 Nederlandse telefoonnummers geblokkeerd. Het gaat om nummers die werden gebruikt om mensen op te lichten.** Om deze vorm van fraude te bestrijden, haalt de toezichthouder de nummers tegenwoordig uit de lucht. Daarin trekt het op met telecombaanbieders, de politie en het Openbaar Ministerie.

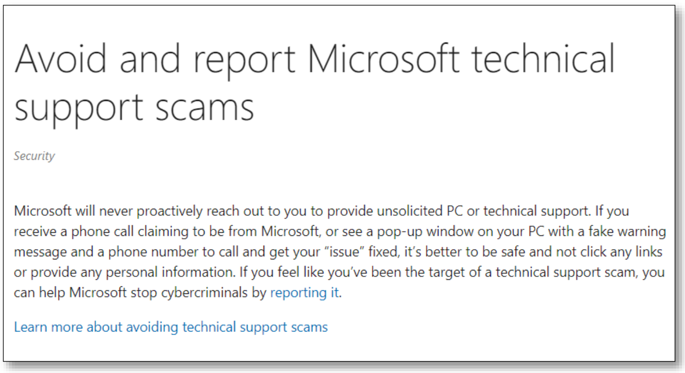
Bron: AD: 19-02-2020

[**ACM tackles helpdesk fraud: 100 phone numbers off the air**
The Netherlands Authority for Consumers & Markets (ACM) tries to tackle fake helpdesks by taking 'bad' numbers off the air.
In the meantime, 100 Dutch telephone numbers have been blocked. These numbers were used to scam people. In order to combat this form of fraud, the regulator now takes those numbers off the air. In this, it collaborates with telecom providers, the police and the Public Prosecution Service.]

Taking out a phone contract with a telecom provider or buying a SIM card is not the only way to use a telephone number. Fraudsters can also use spoofing. This means that it is technically possible to make it look as if they are calling from someone else's phone number. During the project, the possibility of tracing calls made with 'fake' telephone numbers has been looked into. However, this has turned out to be very complicated from a technical point of view due to the - often international - nature of such telephone calls. Thanks to good cooperation between the telecom providers, they are now able to block some of the 'spoofed' telephone calls.

## Microsoft

Microsoft monitors developments through its own notification website 'Avoid and report technical support scams'. This website provides prevention advice and information on what to do if the fraud took place.



Avoid and report Microsoft technical support scams

*Security*

Microsoft will never proactively reach out to you to provide unsolicited PC or technical support. If you receive a phone call claiming to be from Microsoft, or see a pop-up window on your PC with a fake warning message and a phone number to call and get your "issue" fixed, it's better to be safe and not click any links or provide any personal information. If you feel like you've been the target of a technical support scam, you can help Microsoft stop cybercriminals by reporting it.

Learn more about avoiding technical support scams

In addition, Microsoft acts very actively against the fraudsters from its own offices in the country concerned, by reporting them there and by supporting the local police in criminal action if requested.

## Banks and TeamViewer

An intervention that is highly desirable is the linking of the use of a Remote Access Tool and the detection system of the banks. Options to include an extra warning in online banking that makes potential victims extra alert when transferring amounts are also being explored.

# Results expressed in figures

- ➢ Registrations are steadily increasing again after a long period of decrease since Q2 2020.
- ➢ Total damages decreased by 59% compared to 2017 and average damages decreased by 62%. Here again, however, the loss amounts have been rising steadily since Q2 2020.
- ➢ There is as yet insufficient insight into the revenue model. Payment with the use of gift cards has increased.
- ➢ In recent years there has been a shift between sub-MOs. Being called' has decreased and 'Helpdesk search' has increased. In the last two months of 2020 it is visible that being called' is on the rise again. Pop-up messages remain unchanged.
- ➢ The age category of most victims has not changed and is between 60-79 years of age.

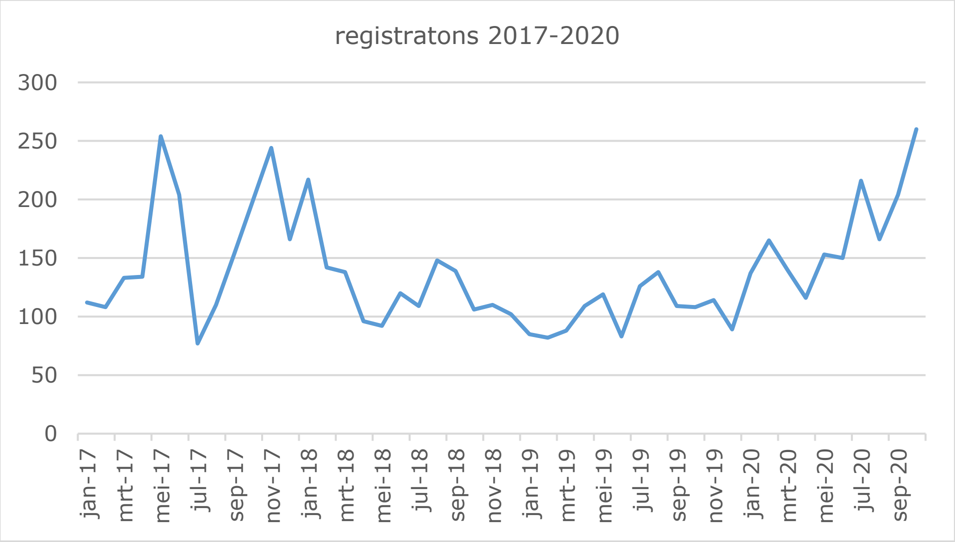
**Development of Registrations**

- *Since 2017, the number of registrations (reports and official reports) of Tech Support Scam in the Dutch police systems has been monitored. After the start of the coalition, a number of partners also provided data to support the quarterly reports delivered since July 2019. In order to provide insight into the developments in the longer term, it was decided to only use police data in this section, as these have been kept up to date since 2017.*
- *The end date for the data below is 31 October 2020, because the final meeting will take place mid-December.*
- *For 2020, the months of November and December have been estimated on the basis of this year's average.*

The development of the number of registrations was as follows:

| Year | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|
| Number of registrations | 1.933 | 1.540 | 1.807 | 2.116 |

In recent years there has been a decrease in the number of registrations, but by mid-2020 this number has increased again:



[translator's note: jan = January, mrt = March, jul = July, sep = September, nov = November]

As mentioned earlier, criminal investigations are hampered by the large international component in this form of cybercrime. Collaborating with countries such as India, for example, is time-consuming and hardly any influence can be exerted on progress. As a result, there is limited insight with respect to offenders and it is therefore difficult to identify the exact cause of this increase since March-May 2020. However, there are a number of possible explanations:

- Since February 2020, it has been possible to report Tech Support Scam digitally. This makes it easier for victims to report to the police.
- From March 2020, the world became increasingly locked up by COVID-19. Just as in the Netherlands, there was also a lock-down in India. However, according to news reports, India quickly relaxed these measures for the IT sector, and it is likely that call centres were also included. Another consequence of COVID-19 is that the public is more active online. Programs need to be

updated so that people look for help desks sooner or believe that, if they are called, there could indeed be a 'hack', as the scammer claims.

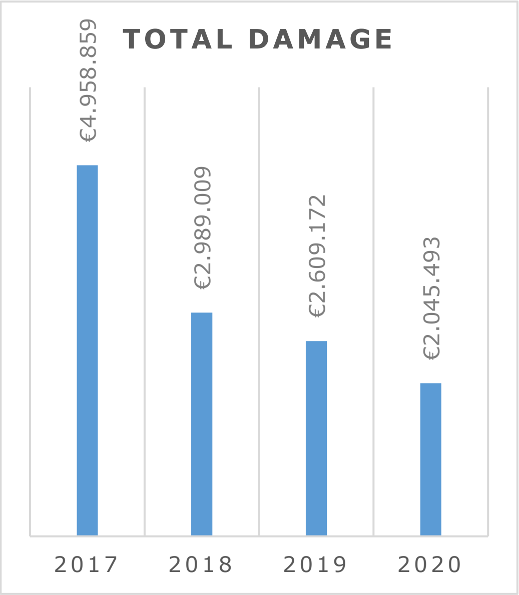
- Reduced media attention for this form of fraud. In recent months, more fraud techniques have been applied to the general public, such as bank help desk fraud and buying and selling fraud. Attention has also been drawn to this in the media. As a result, there has been less attention for Tech Support Scam recently.
- Through Europol, Tech Support Scam appears to be an emerging phenomenon in countries such as Switzerland and Finland. This implies that this form of fraud is and remains a popular form of fraud.

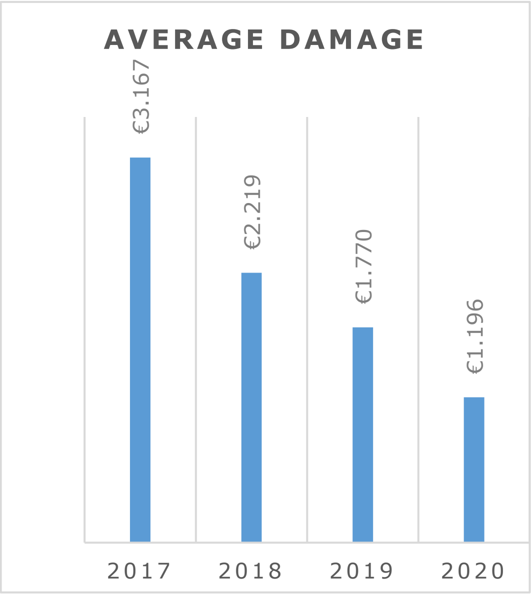
**Development of loss amounts and cash-out**

At the time of the signing of the Declaration of Intent, the estimated damage in 2017 was close to EUR 6 million. By mid-2018 the damage was found to be slightly lower. On the basis of the final figures from 2017 to the present, total damage decreased by 59%. The average loss amounts decreased by 62%.

There was some discrepancy between the information regarding the loss amounts provided by the participating banks and that provided by the police. In most cases, the total loss amounts of the banks are higher than those of the police. This can be explained by the low willingness to report. One might assume that the police do not take any action if an official report is made and people therefore fail to do so. The bank is informed in almost all cases because there are still possibilities, for example, to block the account or a transaction. As it has now been possible to report digitally to the police since this year, this is also intended to increase the willingness to report and to provide a more complete picture of the scope.

The graphs below show the police figures:





During the operation of the Declaration of Intent, hardly any insight was gained into the revenue model. In many cases, the victim's money is immediately transferred to a company, often bona fide, where, for example, prepaid cards are purchased. As a result, the criminal proceeds disappear into anonymity and can no longer be traced.
It has also emerged that transfers often do not take place all at once, but through several transfers. It is likely that this has to do with bypassing the fraud detection systems of banks, for example. At the time of the start of the project, Western Union and MoneyGram, among others, were mainly used to spend the criminal proceeds. On the basis of our information, these companies are hardly used any more. A lot of use was also made of the purchase of bitcoins. Recently, it has become apparent that this has decreased considerably via the cryptocurrency companies affiliated with the Verenigde Bitcoinbedrijven Nederland (VBNL), which can mainly be traced back to a number of disruption measures carried out, such as improving due-diligence.

The information shows that payments via gift cards (such as google playcards, ITunes credit, call credit) have increased significantly. Contacts have therefore also been made with the providers of these cards in order to explore the possibilities of disrupting this part of the criminal process as well.

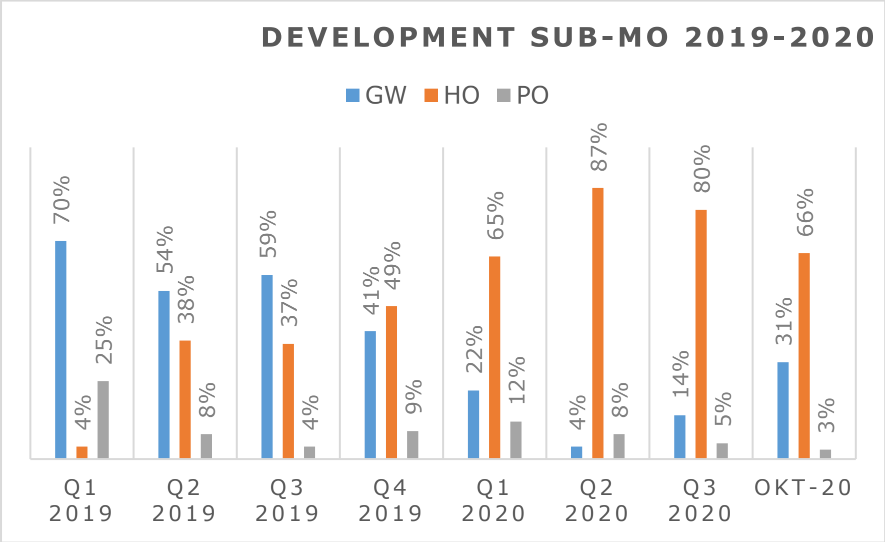
Logical reasoning shows that a conversation between the fraudster and the potential victim takes on average between one and three hours, as far as there is insight into this. This, combined with the average amount of loss, means a high hourly revenue. This is quickly earned and, for a country such as the Netherlands, it will amount to almost EUR 2 million in 2020. If this is compared to the general fact that capital and labour are relatively cheap in a country such as India, for example, Tech Support Scam has a robust revenue model and will therefore not disappear any time soon.

**Development (sub-)MO in combination with average loss amounts**

The data (92% scored) showed that the sub-MO 'being called' has decreased. The tipping point was found to have occurred in Q4 2019. Subsequently, the sub-MO 'helpdesk search' increased.

In 2020 it appeared that 'being called' was steadily increasing again and 'helpdesk search' was decreasing, but still significantly higher than the other two sub-MOs.

Tech Support Scam via a pop-up message remains invariably low.



Based on the 2020 figures, it appears that the average loss amount for the sub-MO 'being called' is the highest, namely € 2,759.77. Followed by sub-MO 'pop-up' with € 944.60 and sub-MO 'helpdesk search' with € 566.92. These figures may be slightly biased because, despite the fact that there was loss, the amount was not always entered in the official report.

It has not been possible to find out why the loss amounts of the sub-MO 'being called' are higher than those of the other sub-MOs. This requires information only known to the offender and this is lacking for the aforementioned reasons.

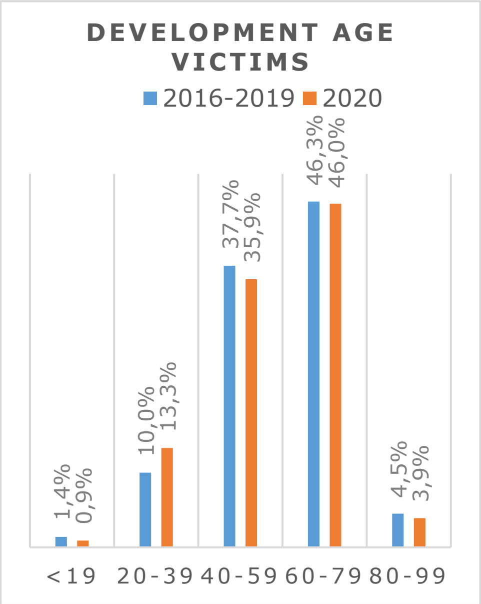
Finally, it is noteworthy that there is an increase in the number of Dutch-speaking helpdesks that also offer technical support. The most remarkable thing is that in a few cases when the victim indicates that he or she does not understand the English language, he or she is put through to a Dutch-speaking person. This could mean that there is cooperation with Dutch-speaking people.

**Development age victims**

This graph shows that the age of the victims has hardly changed in the recorded period. As with other cybercrimes, the elderly are often the victims, as is the case with Tech Support Scam.

It has also been investigated whether there is a link between the age categories and the various sub-MOs. This showed that especially elderly people aged 60 and over are more likely to encounter pop-up messages than in the other age categories.

For both, the work carried out for this project has not led to any research into the underlying reason for this. A possible explanation is the unfamiliarity with the dangers of the Internet of people of this age group. For this report, however, it goes too far to elaborate on this. At the time of this collaboration, a conscious choice was made to focus on action-oriented measures and less on in-depth research.



## Social engineering[4]

Offenders of the Tech Support Scam use 'social engineering', which explains the 'success' of the crime. Social engineering is an attack technique that attempts to

[4] In-depth analysis Tech Support Scam, Jildau Borwell and Kirsten Bos-Riepma

gain access to systems and confidential data of individuals through **deception** and **persuasion**, and to make them actively participate in the crime (Bullée et al, 2018[5]). The fraudsters mislead their victims by pretending to be someone else.

For example, they assume the identity of a help desk employee, technician or security expert; roles generally trusted by people. This increases the chances of the victim going along with the fraudster's story.

Recorded images show that victims have to carry out various tasks, that the caller also searches through the computer and, at the same time, calmly continues to talk. It is noteworthy that the victim has to enter the code for internet banking several times, but is hardly aware of this because of the many actions. In 2009, Stajano & Wilson described this as follows[6]: when people are distracted by certain things and focus on them, all sorts of things can happen around them without them realising it. People focus on what is most interesting to them and on what seems to be the most important action. This also means that this can be managed by the fraudsters.

# Conclusion

The main objective of the Declaration of Intent has been achieved with the reduction of the loss amounts[7]. The uncontrolled growth of the phenomenon in the Netherlands has been halted. The number of victims is at a stable level. The average loss per victim has more than halved during this period.

A better information position has been created in cooperation with the various partners. As a result, developments and trends could be identified more quickly and, where possible, interventions and barriers could be put in place.

However, a profit warning is that in the second quarter of 2020 there has been an increase in the number of registrations and the loss amounts. Dutch-speaking helpdesks in relation to Tech Support Scam also seem to increase. This implies that with the increasing digitisation, this form of cybercrime cannot be eradicated and will continue to develop.

As criminal investigations are complex for the time being due to, among other things, the international component, it is hardly possible to prosecute offenders. The opportunities in the Tech Support Scam approach are therefore mainly to put up barriers in technology and in preventive measures for victims in the Netherlands. However, it will be necessary to continue to focus on connections with India, because this country still seems to play a major role in this form of crime.

Together with the current partners of the Declaration of Intent, the most feasible interventions have been tested and, if possible, set in motion. This means that there is no need to extend the Declaration of Intent for this reason. However, the participants have indicated that they very much appreciate the network that has been set up. This partnership will continue to be very valuable in the future, not only for tackling Tech Support Scam, but also for other cybercrimes. This partnership can, for example, be important in tackling bank helpdesk fraud, friend-in-need fraud, or payment request fraud.

[5] Bullée, J. Montoya, L. Junger, M. & Hartel P. (2018). The success of social engineering. *Tijdschrijft voor Veiligheid,* 1-2, 40-53.

[6] Stajano, F. & Wilson, P. (2009) Understanding scam victims: seven principles for systems security. Cambridge: University of Cambridge

[7] According to the Declaration of Intent, the main objective of the project is 'That the Parties aim to have the Tech Support Scam, in its current dangerous form, eradicated in the Netherlands by the end of 2020 at the latest'.