2021

Trend report Phishing

TIETOEVRY FINANCIAL CRIME PREVENTION

Introduction

TietoEVRY Financial Crime Prevention (FCP) is a leading Nordic center for transaction monitoring for the banking and financial markets in the Nordic, Baltics, and Northern Europe. FCP provides security services to detect and end the misuse of card and payment information to over 80 enterprises in 11 countries. Through FCP's systems, billions of transactions are monitored yearly, and more than 100,000 fraud cases are detected each year. With a unique insight into the trend development of financial crime, the systems help to reduce financial loss and strengthen TietoEVRY's customers' reputation.

TietoEVRY Financial Crime Prevention regards it as its responsibility to help prevent financial crime for all the public community and has for the first time prepared a public trend report to share useful knowledge with other private and public actors

The purpose of the report is to contribute to increased knowledge about phishing scam methods. We want to provide the reader with insight into the scope of the fraud methods and what consequences they may have for the victims. In addition, we will assess further development.

Phishing is not a new type of fraud, but the method has increased significantly in recent years. Compared to other types of scams, victims of phishing are often hit harder financially. With high profits and increasingly advanced methods, it is natural to assume that this fraud method will develop further into several new variants.

By sharing its experiences with this growing fraud method, TietoEVRY wants to contribute to increased cooperation in the fight against financial crime. Cooperation increases the possibility that preventive measures will have an effect and increase the sense of security in the population.

Cecilie Johnsen
Head of Investigation
TietoEVRY Financial Crime Prevention

400 percent increase

Phishing is a form of social manipulation and is a global threat to both enterprises and individuals. The attacks are mainly carried out by organized criminal networks using advanced methods. The complex structures of criminal networks make it challenging to prosecute and stop criminals, and profitability is high.

An increase of almost 400 percent of phishing cases was registered in 2020.The technological development, the introduction of strong customer authentication, high profitability and increasingly professional fraudsters are all strong drivers in this development. So far, there is little indication of a similar increase in 2021, but this can still not be ruled out.

The trend report describes selected phishing methods and provides a future-oriented assessment of these. The selection is based on severity and expected negative development. By publishing the report, TietoEVRY Financial Crime Prevention wishes to contribute to a common situational understanding of the crime challenges facing society in this area. The purpose is to create a good foundation for cooperation in the work of prevention and the fight against financial crime. The report is based on international information from the analysis tools of TietoEVRY Financial Crime Prevention and from external sources.

Likelihood

The assessments form the basis for prioritizing effective measures forpreventing and combating phishing. Assessments of the future involve a certain degree of uncertainty and are reflected by the probability yardstick. The assessments are national and valid for up to one year.

Assessments always involve a certain degree of uncertainty. To handle this in a standardized and structured way, probability words are used.

National Standard	Description	Percentage
Very likely	Very good reason to expect	Very high (>90%)
Likely	Reason to expect	High (60-90%)
Possible	As likely as not	Medium (40-60%)
Not likely	Little reason to expect	Low (10-40%)
Very unlikely	Very little reason to expect	Very low (<10%)

«An increase of almost 400 percent of phishing cases was registered in 2020»

This is phishing

Phishing is a form of social manipulation in which the scammer tries to trick someone into taking action. The scammers “fish” for sensitive information that is used to commit financial crimes for profit. The most common methods are through SMS, email, and telephone, where the fraudsters pretend to be credible recipients of sensitive information. A typical credible recipient can be a Postal Service, Netflix, or Spotify.

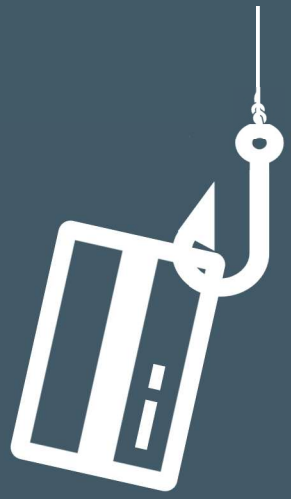
Social manipulation is the art of stealing sensitive information and values from a user with the help of social skills. It can also be used to influence a person's actions. A classic example is that a hacker pretends to be an IT consultant who is to perform maintenance on the user's computer and through this, illegally gain access to usernames and passwords.

Phishing affects victims differently; this is an example of what phishing can look like in practice.

Lisa (25) has participated in a competition on social media to win a speaker Lisa is contacted by the company on social media, informing her that she is the lucky winner. Lisa is informed that the speaker will be sent by post, which entails a shipping fee of EUR 4. Lisa follows the inquiry instructions, entering the card information and verifies the purchase with her BankID. What Lisa does not know, is that by doing so, she provides the scammers with sensitive information they need to clear her card.*

Lisa then receives a phone call from an unknown number, claiming to be from the bank. The bank says that Lisa has been exposed to fraud and that they need her login to BankID to be able to help her further. Lisa is frustrated and needs the help she can get, and therefore provides her personal and BankID information. Once this information has been provided, the fraudsters gain access to Lisa's account and can therefore empty the savings account by transferring money to the checking account and emptying the card.

Lisa’s story is fictional but is based on real events. History shows how easily scammers can gain access to sensitive information and how hard the victims can be hit. The fraudsters rush to clear both the card and the account before the fraud is discovered.



Sensitive information is information that can be used by criminals to steal the victims’ identities or gain access to financial services in the victims’ names. This can be, for example, BankID* (A method used for two-factor authentication), card number, CSV-code, social security number or password.

Well-known phishing methods[4]

E-mail-phishing

The method is often referred to as "spray and pay". The scammers make a fake copy of a known website or service, and then send out a large number of emails to arbitrary recipients.

Spear-Phishing

This scam focuses specifically on individuals in a business. The scammers often use personalized e-mails so that the victim thinks the message is from a colleague, supervisor, or someone they know.

Smishing

In SMS phishing, also referred to as "smishing", text messages are used to scam the recipients.

Vishing

Phone phishing is often called "vishing". Here, the scammers contact the victim by phone. An automated voicemail like an inquiry from a bank or public service is often used.

Spoofing

Spoofing is a method where the scammers hide the number they are calling from and make it look as if you are contacted from a domestic number or a secure IP address.

More methods can be found here: Pandasecurity.com

Trend development

TietoEVRY registered in 2021 an increase of almost 400 percent in the number of phishing cases. There are currently few indications that there will be a further increase in 2021, but this can still not be ruled out. In the period January to September 2021, TietoEVRY Financial Crime Prevention stopped over 5,500 phishing attempts. More than EUR 4.1 million was prevented from falling into the hands of organized criminal networks. Based on available information, it is considered *very likely* that individuals and companies will be exposed to various forms of phishing in the future.

> "In the period January to September 2021, TietoEVRY Financial Crime Prevention stopped over 5,500 phishing attempts. More than EUR 4.1 million was prevented from falling into the hands of organized criminal networks"

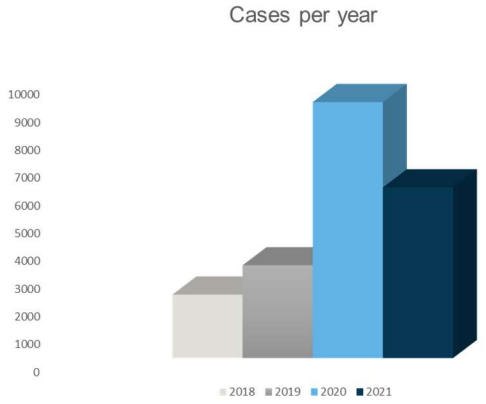
Many recent phishing attempts are linked to money transfer services, and the financial losses are potentially large in cases where fraud is not stopped in time.

Consequences for the victims

Many are tricked by scammers despite warnings and information about various scam methods and trends. The scammers work at a high pace and gain control over the victim's PC, debit card or bank account within a short time. Since the victim has provided sensitive information, the fraud is difficult to detect and the possibility of stopping the fraud is considerably reduced.

Phishing is a particularly harmful form of fraud because criminals often gain access to a lot of information about a single customer or person – not just a debit or credit card. Websites used in fraud attempts are mainly merchants with largely legitimate transactions, which makes it more difficult to distinguish fraud from genuine use. This can reduce the ability to detect fraud.

Banks value passwords and BankID as personal and sensitive data, which the customer is responsible for protecting. When these are stolen, the financial consequences are great, with extensive losses for both the victim and the bank. If the bank's guidelines have been violated, the bank may consider shortening or refusing compensation, leaving the customer to personally carry the loss.



Increased professionalization

The criminals have become more professional, and it is, therefore, more difficult for the victims to detect the fraud. Previously, the scammers mainly contacted their victims by phone from foreign numbers and spoke poor English, which made it easier to suspect fraud. On the contrary, today, the inquiries usually come in written form from a domesic number or email, possibly disguised from a credible enterprise. The message is also well conveyed linguistically, reducing fraud suspicion.

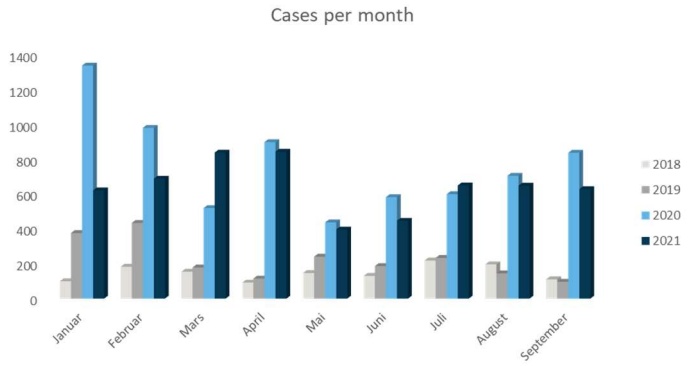
The complexity increases as the fraudsters continuously change and develop their methods as the banks introduce new countermeasures. At the same time, trade and value flow across national borders is an advantage for criminals. It creates an opportunity for scammers when they can sit in another continent and scam Europeans for millions, without having been in Europe.

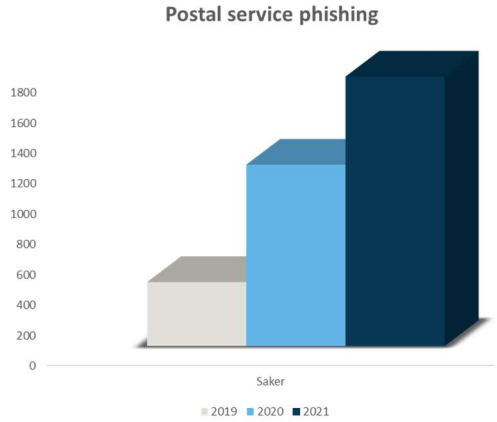
Scammers ally with locals, both to write in the domesic language, but also to understand local victims better. Locals are contacted and hired to translate fraudulent texts that, for example, are to be used in fake Facebook competitions[1].

In some cases, phishing victims provide payment information despite sensing that the email address is strange. One of the reasons for this may be that the fraudsters use apparently small amounts that the victims pay and verify the purchase with strong customer authentication, for example BankID. These small amounts are used as a tool to reduce suspicion of fraud and fear of financial loss. What the victims are not aware of is that when the amount is paid and verified with BankID, the fraudster gets access to a card or account, which can lead to a significant financial loss for the victim.

Phishing trends

The figure below shows the number of registered phishing cases in the period 2018 to 2021.





The postal service

Postal service phishing means that the fraudster pretends to be from the national postal service to gain access to personally sensitive information. From July to August 2020, there was a sharp increase in the number of phishing cases related to logistics services and tracking with the Postal Service as the sender. Despite an increase in the number of cases, we see a decrease in financial losses per case.

Phishing disguised as logistic services, such as The Postal Service, is a major trend. It is *very likely* that especially private individuals will be scammed in the future using this scamming method.
If the increase in these cases continue, it is *likely* that this method will double in 2021 compared to 2020.

[1] Source Dagbladet

Flubot malware

Flubot Malware is a new phishing method that is starting to become widespread[2]. The victim receives an SMS or email from DHL or other postal and logistics services with a request to download and install a "parcel tracking app" via a link on the phone.

If the app is installed on the phone, it will try to obtain personal data, such as logging in to the online bank. It also sends out infected text messages to everyone in the contact list on the phone, which can cause a large spread in a short time.

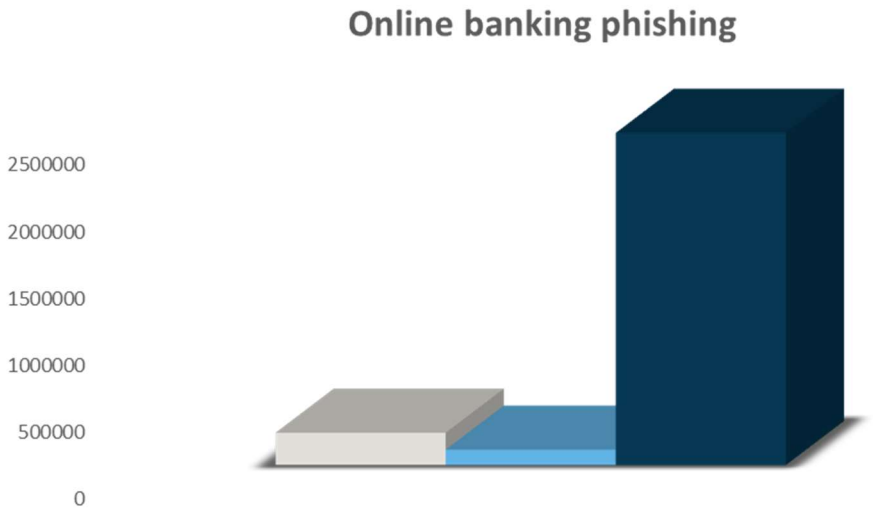
This malware is currently only a problem for Android users, while iOS users who are exposed to this type of phishing, are redirected to a website that has the same purpose as the Android app.

Flubot's weakness is that it has to be installed on the phone. It therefore needs help and approval from the users. TietoEVRY Financial Crime Prevention currently has too little information about flubot malware to be able to say anything about expected development.

Online banking phishing

With online banking phishing, the scammers gain full access to the online bank to transfer funds from the savings account and credit card to the checking account and then empty the account for money. The scammers can also change contact information so that notifications of possible fraud to online banking customers are answered and denied by the scammers themselves.
An increase in the size of financial loss related to online banking phishing has been registered in the last year. An analysis of an attack in January 2021 shows that the fraudsters changed their attacking approach, leading to a greater financial loss in several individual cases. The number of registered cases within online banking phishing is relatively low, but large financial losses are seen per case.

This gives the scammers high profits. From January to May 2021, one large bank alone had 28 cases[3] in which a total of more than EUR 90,000 was stolen. In the largest cases, the victims were robbed of more than EUR 20,000 per case. Based on track record, it therefore appears probable that private individuals could be exposed to online banking phishing, and it is then possible that this could lead to large financial losses if the fraudster succeeds.



[2] Source Tek.no

[3] In these cases, it was mainly SMS or a call from someone who pretended to work for the bank.

Microsoft

Phishing in which the fraudster pretends to represent Microsoft is another known trend. In many cases, the victim provides both bank card information and control of the computer or clicks on a link that locks the PC. These are methods that most often affect larger companies[4], but there are also some cases where private individuals are targeted.

In one case, the victim was in contact with someone who pretended to represent Microsoft and provided information for several credit cards. This resulted in almost EUR 7,000 being stolen.

There is a decline from 2018 to 2020 in Microsoft phishing attempts, and it is *possible* that the decline will continue.

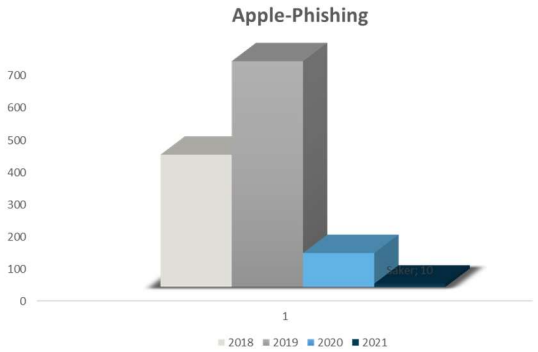
Netflix

A formerly popular scamming method is when the scammer pretends to be representing Netflix. In the period 2018 to 2020, there was a steady decline in Netflix phishing. In 2021, on the other hand, there is so far an increase compared with the previous year.

A review of the cases shows that this fraud method is mainly used in late winter, late summer and around Christmas time. Based on the case development, it is *likely* that Netflix phishing will increase in scope.

Apple

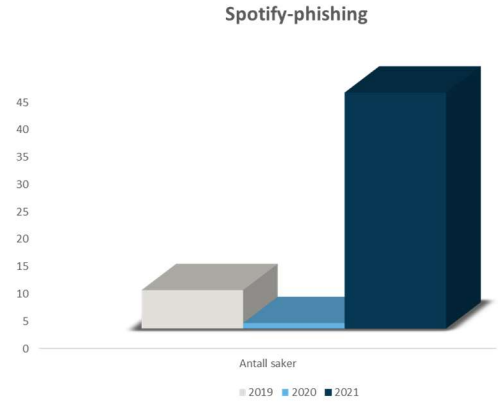
Phishing where the scammer claims to be from Apple, is one of the oldest phishing trends registered by TietoEVRY. The method is similar to that of the postal service and Netflix phishing with SMS or email where the victim is notified that the Apple account has been blocked.
There is a decline in both the number of cases and financial losses, and it is *likely* that this downward trend will continue in 2021. The decline indicates that fraudsters have changed strategy, and that is why we are seeing an increase in other phishing methods



It may seem that the decreasing trend will continue in 2021. One of the reasons is probably better security related to payment confirmation, more vigilant users and better routines for detecting and revealing this type of fraud attempt.The increase we are recording in other phishing methods also indicates that the scammers have changed tactics.

Spotify

There has been an increase in cases related to Spotify phishing in the last year, where the scammers pretend to be from Spotify. In a single case, more than EUR 6,500 was stolen. This is unusually high compared to other cases that use the same method, but not unique. It is *likely* that the number of Spotify cases will continue to increase in scope.



PayPal

The scammer pretends to be from PayPal and then fishes for personal data. The procedure is essentially the same as for other phishing attempts where a known brand is used as the sender. Users

[4] Source The Norwegian Police

are asked to click on a link and provide personal information on a page that the scammers control.

The number of registered cases increased in 2020. We also register that the financial losses in these cases are decreasing. So far in 2021, PayPal is a declining trend, and it is *possible* that the downturn will continue.

Public health services

An attack where the fraudsters pretended to be from a digital health service platform was registered in 2021. The fact that the fraudsters exploit companies and enterprises that are widely mentioned in the media, for example during the pandemic, shows how they follow the news picture and trends in the society in order to exploit these fraud attempts. Recently, the Norwegian Institute of Public Health (NIPH)[5] was tipped off about a fake survey that some residents had received through email, claiming to be sent from NIPH. So far this year, 31 cases of this type of fraud attempt have been registered with TietoEVRY Financial Crime Prevention, most in April.

Targets unemployed people and other vulnerable groups

A new trend[6] is scammers who seek out hopeful people applying for their dream job or who look for vulnerable groups in society to exploit their situation for profit.

The scammers also hack recruitment sites and gather information about potential victims and the jobs they apply for. The victims then receive a fake SMS or email with an invitation to a job interview.

Currently, this fraud method is not registered in TietoEVRY's systems. Information indicates that the fraudsters use transfers between bank accounts in these cases.

Olga scam

Olga scam is a method where scammers target elderly people. In the autumn of 2019, there was a wave of this type of fraud, where older women with names that were common 80 years ago were contacted by phone by someone who pretended to be from the bank. The victims were tricked into giving out information such as BankID and personal passwords to the online bank. Sometimes they were also forwarded to other scammers who pretended to be customer advisers at the bank so that the inquiry would appear realistic and credible. Experience has shown that fraudsters transfer from one account to another and use so-called "mule accounts".

The scammers work specifically towards a particularly vulnerable group. Although the bank warns against this form of Olga fraud, many are still cheated. Fraud practices in which an account is emptied without a bank card being involved, give cause for concern. Until 2019, the possibility of monitoring this type of fraud was limited. TietoEVRY Financial Crime Prevention works continuously with the development and implementation of new security systems to be one step ahead of the fraudsters and the methods they use.

Mules are persons or criminal organizations that, for compensation, transfer profits from criminal acts between payment accounts, preferably in different countries, so that the money eventually appears to be legal.

[5] Source Fhi.no

[6] Source: Dagbladet.no

Looking forward

In this report, TietoEVRY Financial Crime Prevention has presented information on a growing fraud method, phishing. It is very likely that this form of fraud will remain widespread in the time ahead, and that many will experience large financial losses as a result.

The report has also addressed several emerging phishing methods, which in all probability may become more widespread in the time ahead. An important point that emerges from the report is that the fraudsters' methods will continue to adapt to the weaknesses in the market and the development of society. The scammers' adaptations also increase the importance and usefulness of sharing information between parties that fight against financial crime, as well as with society in general.

With this report, TietoEVRY wants to help other players strengthen their work against phishing scams. This should not only include the work done internally in banks, supervisors, and system suppliers, but also communication to consumers.

The report points out that the consumer is the weakest link in the fight against financial crime, especially phishing. An important step in strengthening the work against phishing is therefore to ensure that the consumer has the information and tools needed to guard against this fraud.