Social Engineering

Security

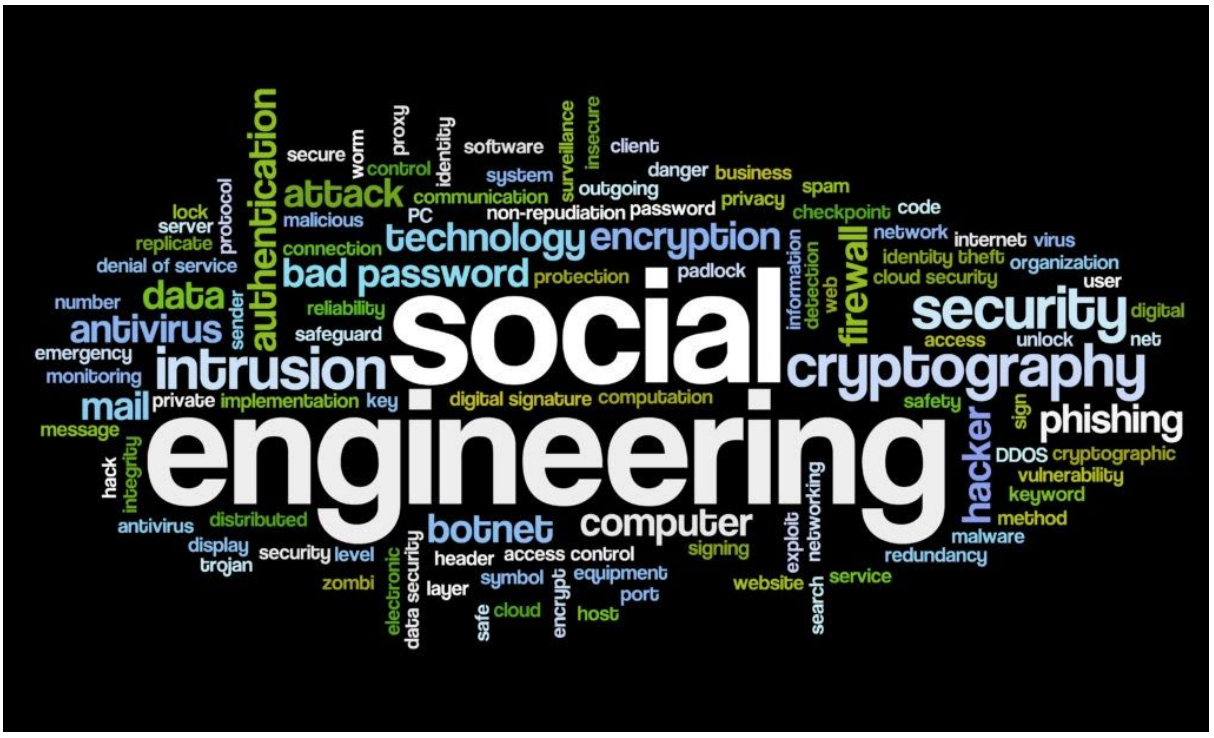


Table of Contents

What is social engineering

Social engineering is a term, describing how a hacker can take advantage of human errors and interactions. The hackers intend is to trick a user into either giving up vital information about their company's IT infrastructure or access to personal information such as login credentials or even gain access to a physical premises.

The attack can be broken down to one or more steps. Usually the hacker would start by gather information about the intended victim, this would be a very thorough examination about the victim. The more information the hacker has on the victim the higher the success rate is of convincing the victim into willingly hand over any information. One of the method the hacker can use is email phishing, where he would compose an email customized with content towards a particular end-user. In the email there would be a link to a malicious website that would be an exact replica of an ordinary page. It could be a website imposter of a banking company. When the end-user types in his/hers login credentials it would be sent directly to the hacker.

Within social engineering there is different types of approaches these are called vectors. One of them is phishing which might be the most common strategy. There are many ways you can receive a phishing attack, either over the phone where a hacker would try to act as someone else to get information, this is called voice phishing or vishing. This could also be done over text message which is called smishing. Another alternative is a method called *typosquatting* where the hacker registers a domain very close to the brand name they want to impersonate, and then creating a website that looks exactly like the brand they are impersonating, an example from the past, is PayPal.com (with a capital i at the end) instead of the real website PayPal.com. And at last impersonation where the hacker would use social engineering in person physically.

Social engineering could be more established than we think

The Social Engineering Toolkit or SET provides the ability to help blackhat hackers, to trick you into giving them your sensitive information, one tool used is the Mass Mailer Attack, which give the ability to send out large amount of scam emails, which will look exactly as a legitimate email from for example your bank, insurance, tax-refund, social media mentioning and more. Mass Mailer also have the ability to full ones email inbox and crash it, if the inbox did not crash, the attack will still be effective because the spam mails will inevitably hide important mails in between the spam mails. Another name for it is E-bombing and SMS-Attack.

This type of attack is typically referred to as phishing attacks or whaling attacks. As both attacks is disguised as reliable sources and emails.

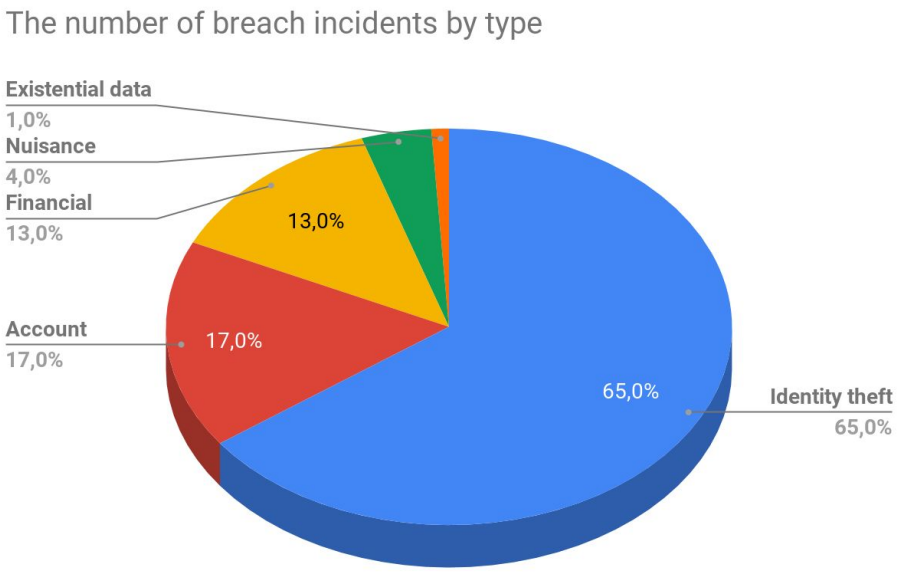
How is a attacked created and executed

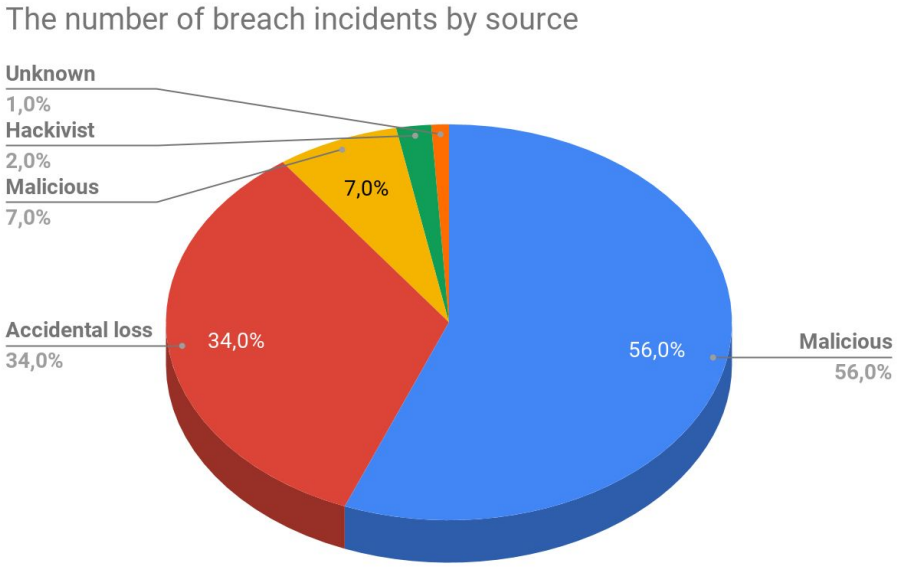
One way a mass mail attack created is as following…

1. First thing first, is to choose the desired attack, which in this case is the Mass Mailer Attack, from the menu bar.
2. Then you get the option of choosing between a mass attack or singling out one specific victim.
3. Choosing the mass attack, will prompt a path for a list of targeted emails.
4. After giving the path, the option for using a gmail account or your own server is displayed. (we are going to use a gmail)
5. All information for the bogus mail will be prompted to be provided, and sent when filled out.
6. In appendix 1 we have screenshots of the legitimate email (left) and the bogus (right).

https://medium.com/@hackersleaguebooks/what-is-mass-mailer-attack-6f205c2d9937 (you need to show me how to do the documentation)

You might think that cybercrime is easy to come around and in these days we are not that exposed to such attacks. But if you look at the statistics for these types of attack the numbers tell a different story. Actually all cyber attacks are relying 98% on social engineering skills[1] you could argue that the damage is unharmful and it isn't worth protecting against but based on the statistics, it takes more than a week for 90% of the financial institutes to regain back access to their data after such attack.



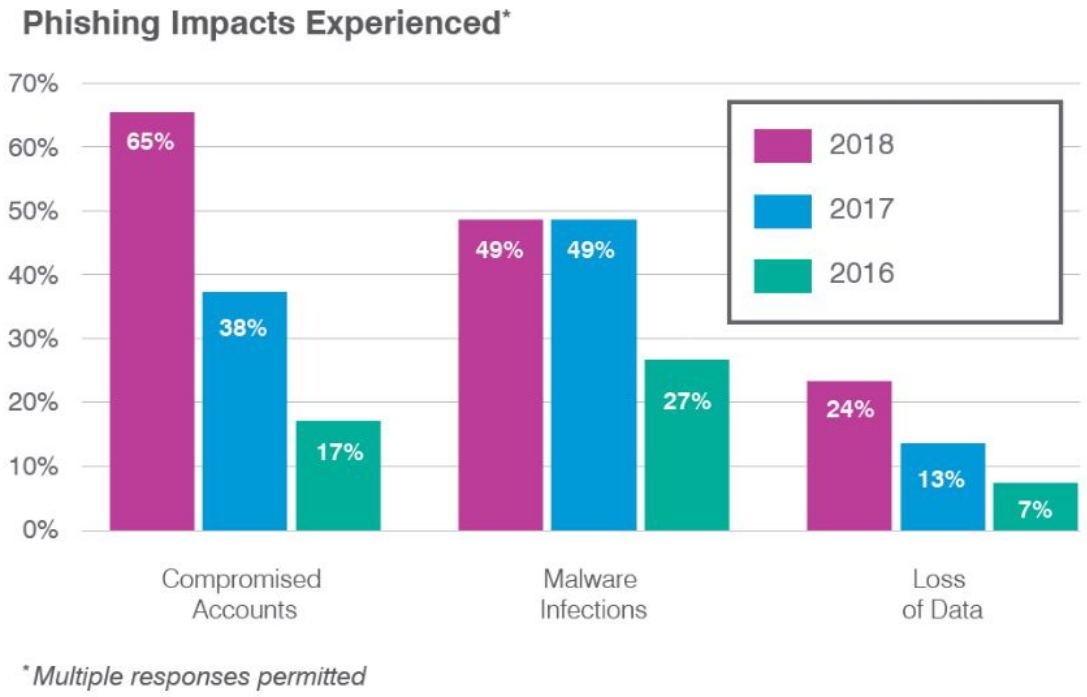


[1] https://purplesec.us/resources/cyber-security-statistics/

What are the statistical numbers of attacks

According to studies(1), 55% of all emails are spam, with the email flow now a days for most people, this statistic is critical. Most of us may be able to spot the most obvious flaws and red flags in emails, but the constant flow of mails wears down our ability to spot the more thorough created spam mails. Sophisticated cyber crime attacks through email is a staggering 91% of all cyber crime attacks(2).

The top tier areas of successful phishing attack are in social media, entertainment, and reward or recognition. The reason why these are the top tier areas, is because the older motivator of *fear and/or curiosity* has caused fewer successful attacks in recent times. the frequency of attacks are now directed more towards *consumer scams* which targets *while on the job* employees personally. When employees use personal devices for work or checking their social networks or keeping up with the news, the lines become blurry.



(3 pic)

According to CyberEdge report(4) from 2017, the numbers of successful attack was 79%, compared to the number of successful attacks in 2014, where it was only 62%, then it rose to 71% in 2015 and then 76% in 2016. Wombat Security's(5) "2019 State of the Phish" report states that around 83% of all companies have reported that they have experienced phishing attacks in the past year. The report

also states that 49% have experienced voice or SMS phishing, where only 4% experienced attacks by infected thumb drives.

In 2018 a study(6) showed 17% of people were victimized by social engineering attacks. That means that almost 2 in every 10 employees, have unknowingly provided attackers with sensitive information. The same study showed that 27% of employees clicked on a link that send them to a bogus website. It also showed that the employees did not hesitate to open unknown files, visit suspicious links, or even talk/chat to attackers.

It takes an average of 146 days(7) for a company to detect a data breach due to email phishing. With that amount of time the attacker would have been able to get everything in your network, or computer. The average lifecycle of a breach was 314 days (from the breach to containment)(8).

According to the FBI, the impact of a social engineering attack can be quantified. Companies have paid 1.6 billion dollars(9), in the period of 2013 to 2017 as a result of successful social engineering attacks. A study released in 2017 “Cost of Cyber Crime Study”(10) showed that there are around 130 security breaches every year and companies pay an average of 11.7 million dollars annually for cybersecurity. The average cost of a data breach is $3.92 million as of 2019(11).

Worldwide spending on cybersecurity is predicted to reach $133.7 billion in 2022(12). Data breaches exposed 4.1 billion records in the first half of 2019(13). The average cost per record stolen is $150(14). The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%(15). Hackers attack every 39 seconds, on average 2,244 times a day(16). Only 5% of companies’ folders are properly protected, on average(17).

(1)https://www.sysgroup.com/resources/blog/statistics-need-to-know-social-engineering

(2)https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

(3)(5)https://www.proofpoint.com/us/corporate-blog/post/2019-state-phish-report-attack-rates-rise-account-compromise-soars

(4)https://cyber-edge.com/wp-content/uploads/2017/06/CyberEdge-2017-CDR-Report.pdf

(6)https://datafloq.com/read/social-engineering-attacks-numbers-cost/6068

(7)https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf

(8)(11)(12)(13)(14)(15)(16)(17)https://www.varonis.com/blog/cybersecurity-statistics/

(9)https://bankingjournal.aba.com/2017/05/fbi-social-engineering-scams-cost-u-s-businesses-1-6b-since-2013/

(10)https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

Is it possible to prevent being attacked?

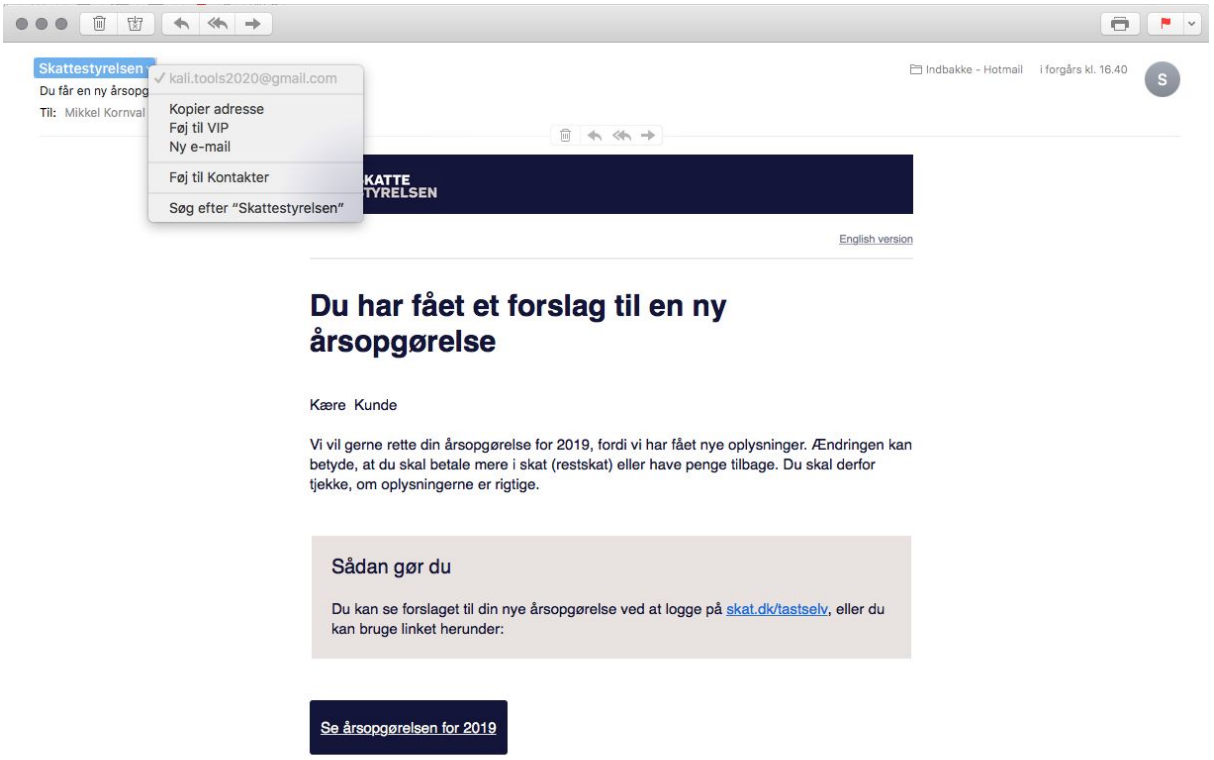
How do you prevent social engineering attacks from happening to you or your company? First and foremost if you ever receive an email from an untrusted contact, the first thing you would like to do is check what the sender domain it is and see if it matches the name of the specific email name. Here should the first red flag occur and you should properly delete the email right away and maybe consider inform your IT department. If the domain name checks out, you could copy and paste the link if there is any to a text application and see if that looks safe to use or if you don't know what to look after ask a competent colleague or your IT department. If you have already clicked the link in the email, you could check to see if it is protected by HTTPS protocol by looking at the url bar. You should see a lock or some kind of confirmation that it is safe so use. Have in mind that some internet browsers don't allow you to open non HTTPS websites such as Google's chrome application.

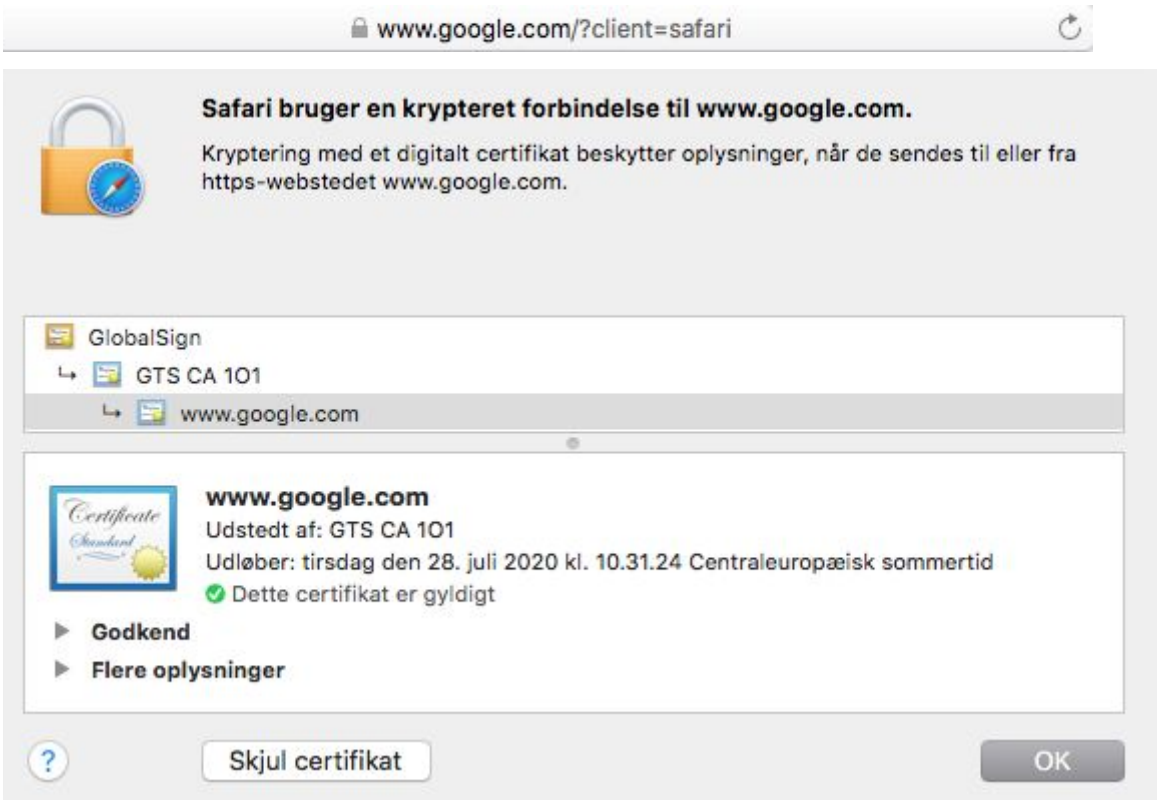
There are many ways to prevent getting hacked but it is hard to prevent getting attacked, therefore always double or triple check the emails you are receiving. Sophisticated phishing attacks is known to use information about your social network, former or current positions through LinkedIn, Facebook or other informative websites, which gives just enough liable information for it to seem plausible to get your non-suspicious attention.

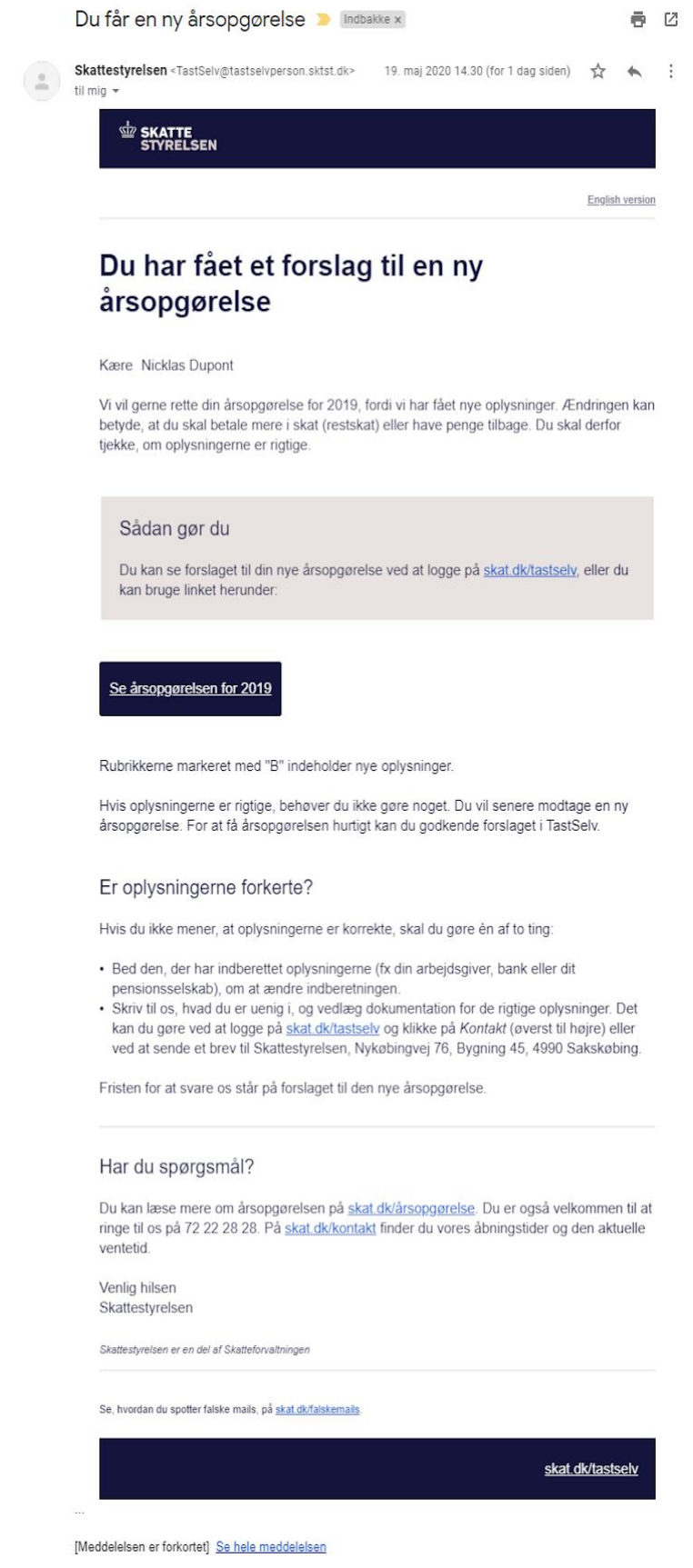
Some email clients have built in security function, take a look at how they work and if possible set the filter for spam mails to high. Changes are that you properly have your information spread out to a lot of devices, be sure to have installed the latest security updates and if your device isn't supported any longer consider getting rid of it or at least remove any sensitive information from it. For better safety you could install a VPN client to make all your data packets encrypted.

Device securing like improving endpoint device security is one way to protect yourself against phishing attacks, this includes encrypt data, monitor connectivity, whitelist applications and block unwanted activity.

https://www.sysgroup.com/services/it-security/endpoint-security




www.google.com/?client=safari
Safari bruger en krypteret forbindelse til www.google.com.
Kryptering med et digitalt certifikat beskytter oplysninger, når de sendes til eller fra https-webstedet www.google.com.
GlobalSign
GTS CA 1O1
www.google.com
www.google.com
Udstedt af: GTS CA 1O1
Udløber: tirsdag den 28. juli 2020 kl. 10.31.24 Centraleuropæisk sommertid
Dette certifikat er gyldigt
Godkend
Flere oplysninger
Skjul certifikat
OK



Du får en ny årsopgørelse Indbakke ×

Skattestyrelsen <TastSelv@tastselvperson.sktst.dk> 19. maj 2020 14.30 (for 1 dag siden)
til mig

SKATTE STYRELSEN

English version

Du har fået et forslag til en ny årsopgørelse

Kære Nicklas Dupont

Vi vil gerne rette din årsopgørelse for 2019, fordi vi har fået nye oplysninger. Ændringen kan betyde, at du skal betale mere i skat (restskat) eller have penge tilbage. Du skal derfor tjekke, om oplysningerne er rigtige.

Sådan gør du

Du kan se forslaget til din nye årsopgørelse ved at logge på skat.dk/tastselv, eller du kan bruge linket herunder:

Se årsopgørelsen for 2019

Rubrikkerne markeret med "B" indeholder nye oplysninger.

Hvis oplysningerne er rigtige, behøver du ikke gøre noget. Du vil senere modtage en ny årsopgørelse. For at få årsopgørelsen hurtigt kan du godkende forslaget i TastSelv.

Er oplysningerne forkerte?

Hvis du ikke mener, at oplysningerne er korrekte, skal du gøre én af to ting:

- Bed den, der har indberettet oplysningerne (fx din arbejdsgiver, bank eller dit pensionsselskab), om at ændre indberetningen.
- Skriv til os, hvad du er uenig i, og vedlæg dokumentation for de rigtige oplysninger. Det kan du gøre ved at logge på skat.dk/tastselv og klikke på *Kontakt* (øverst til højre) eller ved at sende et brev til Skattestyrelsen, Nykøbingvej 76, Bygning 45, 4990 Sakskøbing.

Fristen for at svare os står på forslaget til den nye årsopgørelse.

Har du spørgsmål?

Du kan læse mere om årsopgørelsen på skat.dk/årsopgørelse. Du er også velkommen til at ringe til os på 72 22 28 28. På skat.dk/kontakt finder du vores åbningstider og den aktuelle ventetid.

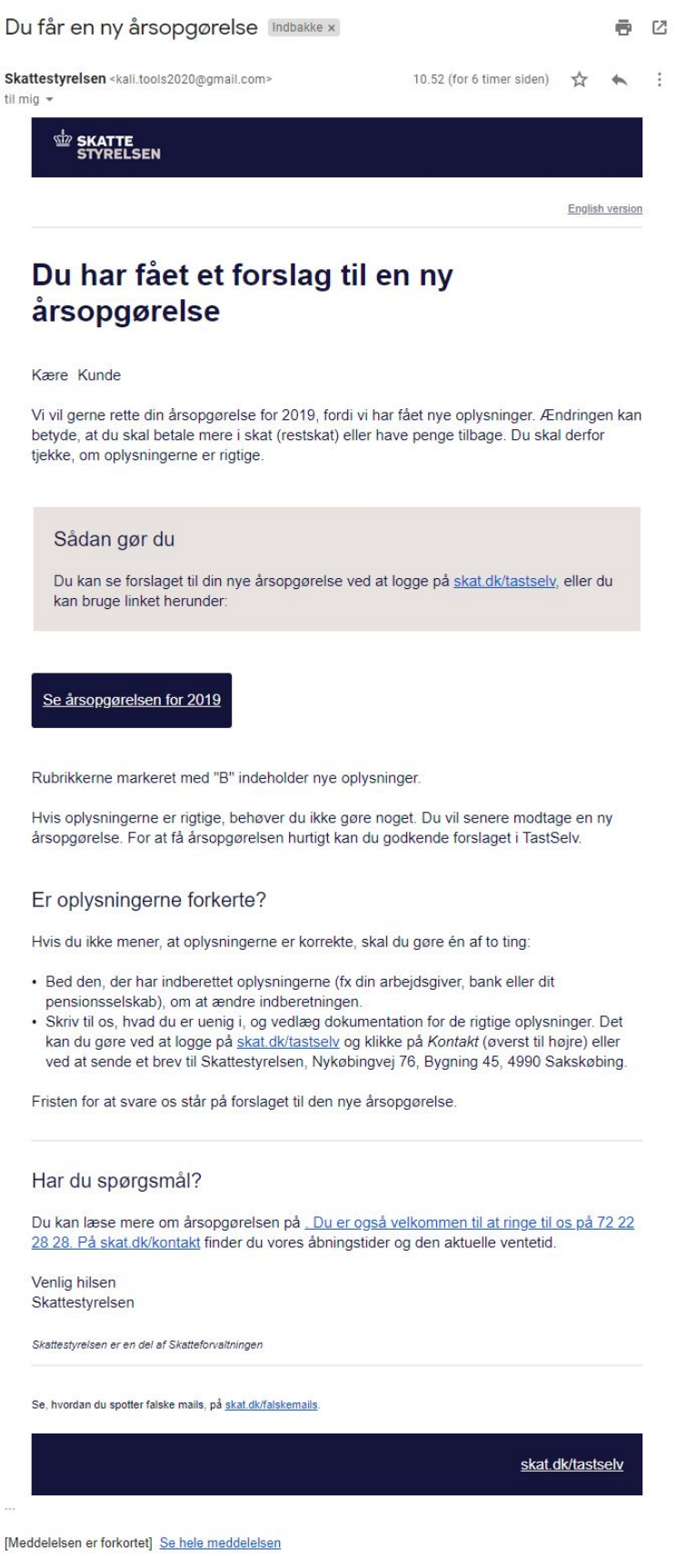
Venlig hilsen
Skattestyrelsen

Skattestyrelsen er en del af Skatteforvaltningen

Se, hvordan du spotter falske mails, på skat.dk/falskemails.

skat.dk/tastselv

[Meddelelsen er forkortet] Se hele meddelelsen



Du får en ny årsopgørelse Indbakke ×

Skattestyrelsen <kali.tools2020@gmail.com> 10.52 (for 6 timer siden)
til mig

SKATTE STYRELSEN

English version

Du har fået et forslag til en ny årsopgørelse

Kære Kunde

Vi vil gerne rette din årsopgørelse for 2019, fordi vi har fået nye oplysninger. Ændringen kan betyde, at du skal betale mere i skat (restskat) eller have penge tilbage. Du skal derfor tjekke, om oplysningerne er rigtige.

Sådan gør du

Du kan se forslaget til din nye årsopgørelse ved at logge på skat.dk/tastselv, eller du kan bruge linket herunder:

Se årsopgørelsen for 2019

Rubrikkerne markeret med "B" indeholder nye oplysninger.

Hvis oplysningerne er rigtige, behøver du ikke gøre noget. Du vil senere modtage en ny årsopgørelse. For at få årsopgørelsen hurtigt kan du godkende forslaget i TastSelv.

Er oplysningerne forkerte?

Hvis du ikke mener, at oplysningerne er korrekte, skal du gøre én af to ting:

- Bed den, der har indberettet oplysningerne (fx din arbejdsgiver, bank eller dit pensionsselskab), om at ændre indberetningen.
- Skriv til os, hvad du er uenig i, og vedlæg dokumentation for de rigtige oplysninger. Det kan du gøre ved at logge på skat.dk/tastselv og klikke på *Kontakt* (øverst til højre) eller ved at sende et brev til Skattestyrelsen, Nykøbingvej 76, Bygning 45, 4990 Sakskøbing.

Fristen for at svare os står på forslaget til den nye årsopgørelse.

Har du spørgsmål?

Du kan læse mere om årsopgørelsen på . Du er også velkommen til at ringe til os på 72 22 28 28. På skat.dk/kontakt finder du vores åbningstider og den aktuelle ventetid.

Venlig hilsen
Skattestyrelsen

Skattestyrelsen er en del af Skatteforvaltningen

Se, hvordan du spotter falske mails, på skat.dk/falskemails.

skat.dk/tastselv

[Meddelelsen er forkortet] Se hele meddelelsen