CENTRE FOR CYBER SECURITY

Threat Assessment

Cyber threat from phishing emails

Cyber attacks initiated through phishing emails are a widespread phenomenon, resulting in loss of money, data and reputation or serious compromise of IT networks.

Table of Content

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

1. edition December 2020.

Key assessment

Cyber attacks initiated through phishing emails are a widespread phenomenon, resulting in loss of money, data and reputation or serious compromise of IT networks with public authorities and private companies. Keeping a high level of threat awareness and introducing appropriate counter measures are thus essential.

- The CFCS assesses that phishing through emails is a persistent and serious cyber threat to all public authorities, private companies and citizens in Denmark.
- Today, most cyber attacks likely start off with a phishing email.
- The CFCS assesses that as much as 80 per cent of the emails organizations receive from senders outside the organization are unsolicited or even malicious and that larger organizations receive phishing emails on a daily basis.
- Phishing is used by cyber criminals and state hackers alike. The CFCS assesses that most phishing emails are sent by organized criminals who also provide infrastructure, tools and services in support of phishing.
- Phishing attacks could potentially have a detrimental impact on society if they target authorities or companies that perform critical functions, provide essential services, etc.
- The CFCS assesses that most phishing emails point to fake websites that mimic legitimate sites. Closing or blocking access to websites can remove the harmful effect of the specific phishing email.

Analysis

The CFCS assesses that phishing via emails poses a persistent and serious threat to all public authorities, private companies and citizens in Denmark.

Communication by email is used by virtually all public authorities, private companies and citizens in Denmark. Without special technical competencies, hackers can use emails to compromise organizations or private individuals, making it attractive for hackers to intersperse fake and malicious emails in the stream of legitimate ones. The CFCS assesses that today most cyber attacks start off with a phishing email.

Most phishing attacks are opportunistic, meaning that everyone with an email account is a potential phishing target.

The volume of phishing emails that creep into organization inboxes is so substantial that attempts at compromise through fake and malicious emails for many organizations are a daily occurrence.

In addition to the direct threat of compromise, phishing also generally erodes the trust in emails, resulting in legitimate emails sometimes being mistaken for phishing.

Phishing
Phishing is an attempt to trick an email recipient into inadvertently passing on personal and other protection-worthy information, or giving unauthorized access to, for example, IT systems.

Often, the perpetrator uses simple social engineering tactics to lure victims into clicking a malicious link leading to false websites or opening malware-infected files.

Phishing emails are often sent as bulk email to a large number of random recipients without being customized to individual recipients.

Spear phishing
Spear phishing is a targeted attempt to trick one or more specific victims into passing on personal or other protection-worthy information, or giving unauthorized access to, for example, IT systems. Spear phishing is conducted through, for instance, email.

Spear phishing often uses sophisticated social engineering techniques to customize the content to a specific victim. Communication is typically customized to appear particularly relevant, convincing and credible to the recipient, for instant by using their name or other personal information gathered through prior reconnaissance.

Even though spear phishing resembles phishing, the key difference between the two is that the victims of the former are not random but handpicked.

Phishing is used across a variety of hackers – from the less advanced cyber criminals, who work alone, to organized criminal groups. Common to both hacker types is that financial gain is their end goal. Phishing is also used in connection with cyber espionage with the purpose of gleaning information of financial, military or political relevance.

Phishing is typically used for:

- Theft of username and password to Internet services such as email accounts, social media, web shops, etc.
- Theft of debit card information.
- Business Email Compromise (BEC) fraud in which the victim is lured into transferring money to criminals.
- Installation of malware on victim computers.
- Establishing a foothold in IT networks as launch pad for further compromise.
- Theft of sensitive or protection-worthy information.
- Theft of NemID information (unique to Denmark).

The information hackers obtain through phishing is exploited by the hackers themselves, is sold or leaked to the detriment of the victim. The information may also be passed on to a third party, for instance in connection with cyber espionage.

The methods used in phishing are also employed in connection with text messages or phone calls, in which case the methods are called smishing and vishing respectively. A common feature between the three methods is a weakness in the underlying technology making it possible for the perpetrator to spoof his identity. Of these three methods, phishing through emails is particularly dangerous to public authorities and private companies. The reason is that the employee email clients are connected to the internal IT network whereby a phishing attack may infect the IT network with malware.

Smishing
Smishing is phishing attempts through text messages. Typically, the text message will try to lure the recipient into entering a website to confirm passwords or debit card information or to download a harmful app. The victim may also be tricked into calling a phone number that the perpetrator will then use to continue their scam.

Vishing
Vishing is phishing attempt through phone calls. The caller may tell the victim that they have won a prize and that they must give their personal details in order to

receive it. The caller may also claim that there are security problems related to the victim's computer, debit card or bank account, and that they must share their personal information or passwords in order for the problem to be solved.

Most emails are unwanted or potentially malicious

Each day, Danish private companies and public authorities receive millions of emails. The CFCS assesses that as much as 80 per cent of such emails are unwanted or potentially malicious. The high volume of phishing emails shows that cyber attacks through phishing are a persistent threat.

Due to the extent of unwanted and malicious emails, most email services and companies use different email filters whose criteria determine whether to let an email through to the recipient, to reject it, or to keep it quarantined until approved by the recipient.

As it can be difficult to univocally identify a phishing email, and to eliminate the risk of rejecting legitimate emails, the filter usually only rejects emails assigned with a high spam or malware score. Consequently, email filters will not be able to intercept all phishing emails.

Tests conducted by IT security companies have proved that as many as every tenth phishing email escapes the standard email filter.

The most common reason for emails to be rejected is that the sender domain or IP address is known for sending unsolicited advertisements or phishing emails. Other emails are rejected as they contain known malware or links to known malicious websites. More advanced filters try to detect yet unknown phishing emails and malware by searching for text, fragments of code or acts indicating malicious content.

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system used by an increasing number of organizations. This system can protect an organization's domains against abuse in phishing attacks. On the recipient side, DMARC rejects emails sent from email servers that are not affiliated with the organization featuring as the sender of the email. This is a tell-tale sign that the sender is not who they pretend to be, suggesting that the email may fall into the phishing category.

Most employers allow their staff to access private email accounts via company computers. Such emails do not pass through the company's email filter. As a result, the company, more or less deliberately, chooses to trust that the public mail service in question uses an email filter and that this filter is effective.

An organization may get an overview of the threat from phishing by looking at the number of emails rejected by its email filter.

Covid-19 is exploited in phishing emails
The Covid-19 pandemic is a case in point of how cyber criminals exploit citizens' curiosity or fear and their thirst for information. The Covid-19 pandemic has thus been the topic of several phishing campaigns and fake websites directed against Denmark.

On 2 April 2020, the L 157 bill entered into force, giving Danish Police the power to order telecommunications providers to block the access to malicious websites related to the Covid-19-pandemic. Subsequently, the CFCS has continually submitted information on phishing websites to the police, resulting in the blocking of more than 30 sites (late September 2020) targeting Denmark.

In addition the CFCS has identified a three digit number of other fake websites trying to lure NemID, debit cards and passwords from Danish citizens. In an attempt to remove these websites the CFCS makes contact to the hosting providers renting out server space to the criminals. Unfortunately this process is often slow and not always successful.

CFCS assesses that in future, cyber criminals will also try to exploit state compensation schemes as a theme in phishing emails.

As more people have started working from home, staff have started using new tools facilitating remote access and online cooperation. Hackers have pounced on this new opportunity, launching phishing campaigns that try to steal access to the tools. As staff are unfamiliar with the new tools, they are easier to scam using phishing emails.

CFCS assesses that overall, Covid-19 has not triggered a general increase in the cyber threat against Denmark, though some of the actors already using phishing have been quick to exploit the pandemic as lures in their phishing emails.

Hackers are often technically skilled and understand human nature
Before a phishing email can inflict the damage intended, it has to pass a minimum of two obstacles, one being the email filter, the other being the person deciding whether or not to click on an attachment.

Hackers know how email filters and humans react to emails. It is thus a constant race between hackers on the one side trying to exploit vulnerabilities and security companies working to detect and block phishing emails and companies training their staff in phishing email detection on the other.

New ways to avoid email filters are quick to spread in hacker circles and via IT security companies in their warnings to the public against the new methods. Below are examples of ways used by hackers to evade email filters:

- Phishing emails are sent from accounts created with free email services. Hackers can simply create new accounts if the old ones are blocked or deactivated by the service provider.
- Phishing emails are sent from legitimate but compromised email accounts that have no previous history of sending unwanted or malicious emails.
- Phishing is sent from botnets – a string of Internet-connected computers and other devices infected by malware, facilitating central control by a hacker. A botnet hides the identity of the email originator, sending phishing emails from domains and IP addresses that have not yet been blocked by the email filter.
- At regular intervals, a phishing website is moved to a new domain that has not yet been identified and blocked by the email filter.
- Malicious files are placed on a legitimate file sharing site. A link inside the phishing email then opens the file when the recipient clicks on the link.
- Malicious files are camouflaged or compressed, for instance in a zip archive, making them not immediately recognisable or analysable to the email filter. However, many email filters quarantine emails containing compressed files until the recipient has accepted them.
- The phishing email contains a link to a legitimate but compromised website that redirects visitors to a malicious website.
- A malicious link is embedded in an attached file or is disguised as a QR code or through a service that abbreviates and changes the name of the link such as Bitly.com.
- The text in the phishing email is inserted as an image, preventing immediate analysis by the email filter.

Hackers may know you better than you think

Spear phishing is used for targeted attacks on specific individuals, groups or organizations of special interest to the hacker. Instead of sending out a large number of identical emails, the attacker customizes the attack to fewer but more specific recipients with the hope that more of the recipients will open the email. Spear phishing is used in, for example, BEC fraud and cyber espionage.

Spear phishing generally requires that the sender has gathered some knowledge about the recipient such as personal or professional circumstances and interests. Such knowledge can be obtained by searching for information on social media and websites. Occasionally, the hacker obtains knowledge of the recipient through more aggressive techniques. Citing shared interests or mutual professional experience, the hacker manages to create a relationship of trust with the victim. Contact to the victim may be initiated through social media such as LinkedIn and Facebook.

A spear phishing email may contain information and links to subjects that are of interest to the target – professionally or personally – while links and documents may be false and malicious.

The cut-off point between phishing and spear phishing is not always clear. The most obvious feature separating spear phishing and phishing is that the victims of the former are not random but carefully selected.

Sextortion emails

Sextortion emails fall into the group of emails that resemble spear phishing but whose victims are random. Typically, the hacker has gained access to leaked email addresses and associated passwords of totally random individuals. The hacker references a genuine password associated with the recipients' email accounts.

Subsequently, the hacker claims to have recorded compromising footage of the recipient through their webcam. The leaked password is intended to convince the recipient that the claim is true. The hacker then threatens to leak the footage if money is not transferred. Unless the email does in fact contain footage of the recipient, it is in all probability a bluff and the hacker thus holds no compromising footage.

Some hackers target their spear phishing emails against executives or IT staff. The former can be exploited in BEC fraud campaigns, while the latter often have administrative rights, making it easy to install malware on their computer. IT staff may also have access to network tools that the attacker can exploit to move deeper into the organization's network once the malware has been installed on the victim's computer.

Hackers try to hide red flags in phishing emails

As phishing awareness is generally increasing, alert employees are often able to recognize less sophisticated phishing emails. As a result, many hackers have grown more creative, shifting to so-called social engineering tactics to make the recipient overlook any red flags in a phishing email.

Social engineering is an attack technique in which the attacker uses psychological techniques to win the trust of the victim, who can subsequently be manipulated into acts they would otherwise not have performed, including unknowingly passing on sensitive or classified information. Phishing emails often exploit a person's habitual behaviour, trust in authorities, curiosity or helpfulness.

Examples of social engineering in phishing emails

The email is in perfect, or almost perfect, Danish, making the recipient feel at ease and adding to its air of legitimacy.

The email purports to be from a private company or public authority that the recipient trusts, a trust that will then extend to include the email. Email was invented in a time when IT security was not yet a priority. Consequently, it is possible to enter a fake sender address in an email.

The email contains images and logos of established organizations, creating the impression of a genuine identity and creating a sense of trust in its content.

Links and attached files have names that seem innocuous, cloaking their true purpose of directing the user to a malicious website. Many users are unaware that the name of a link can be different from the name of the website it points to.

The content requires immediate action, and the recipient is threatened with negative consequences if they do not react without delay. The hope is that the victim does not take time to assess the authenticity of the email.

The content appears very alluring, sensational or scary, evoking strong emotions that make the victim react without thinking.

The content refers to a subject that has a lot of media attention. The hope is that the recipient will be curious enough to ignore any warning signs and click on attached links or documents.

The email is short. The headline ”Look here” or ”Is this true?” in combination with a link or document plays on the curiosity of the recipient and contains fewer elements that may rise red flags.

Phishing is a shortcut to malware installation

Three techniques in particular are favoured for compromise of company IT networks: compromise of usernames and passwords, hacking of company Internet-facing systems, and phishing. The CFCS assesses phishing to be the most common technique. It is a channel for both targeted and opportunistic attacks.

Ransomware attacks are often set off by a phishing email. This was the case when in April 2020, the company Danish Agro became the target of a ransomware attack in which the initial attack was conducted through a phishing email sent from an account belonging to a compromised sub-supplier.

Unless the hacker already has access to a valid username and password, giving access to the company’s IT network, it will typically be easier for them to send malware via a link or an attached file in a phishing email than to scan an IT network for open ports and then hack their way into the company through any vulnerabilities in the underlying software. In the latter method, the attack surface may be limited, requiring sophisticated hacker competencies.

Conversely, phishing provides an extensive attack surface, corresponding to the total number of work-related and private email accounts that employees can access from their work computers. Moreover, a phishing email will often pass undetected through a perimeter firewall because the ports necessary to allow email traffic are open.

If an employee inadvertently opens a phishing email containing malware that can exploit a vulnerability in their computer, this will, as was the case with Danish Agro, often be but the first step in the cyber attack. The initial malware can create a

backdoor to the computer that can subsequently be used by the hackers to download additional malware and hacking tools, or the access can be sold to other hackers.

State hackers also use phishing

Phishing is an effective way of gaining unauthorized access to a computer or Internet service, making it an attractive tool for states, for instance in connection with cyber espionage campaigns. The use of phishing is typically restricted to the initial stages of a cyber attack. It is only when the hacker has gained access to a computer in the targeted IT network that the advanced hacker tools will be deployed, giving the attacker a backdoor to the IT networks and the chance of disguising their presence and entering deeper into the IT network.

Cyber attacks, including phishing emails, by state actors will typically have the goal of collecting information of economic, military or political importance to the country. Though cyber espionage may target all types of public authorities and private companies, it mainly targets public authorities and organizations involved in foreign and defence politics; critical and research-heavy companies and institutions; and Danish representations abroad.

State actors often have access to significant resources, enabling them to launch targeted and large-scale phishing campaigns. A case in point is the 2018 indictment by the US Ministry of Justice of nine Iranians with ties to the Iranian state for their alleged orchestration of spear-phishing attacks against 320 universities in 21 countries, including Denmark.

According to the indictment, the Iranians targeted more than 100,000 professors worldwide with spear phishing emails in the period from 2013 to 2017. The content of the emails related to articles written by the recipients and contained links to websites that were of relevance to their research. In reality, one of the attached links led to a false login page resembling the one used by the recipient professor's university. This enabled the attackers to steal login credentials and gain access to the university network.

Back in 2015, the Danish Computer Security Incident Response Team (DKCERT), which monitors security on the research net, detected a phishing attack that was in all probability part of the above phishing campaign. The attack resulted in the compromise of passwords belonging to 25 employees at Danish universities.

Phishing emails may come from business partners

The CFCS knows of several cases in which compromised email accounts belonging to Danish companies have been abused to disseminate phishing emails to their business partners in Denmark.

It is hard for the recipient to detect the fraud as the phishing email seems to originate from an employee or company known to and trusted by the recipient. This facilitates spread of the attack from a compromised email account in one company to an email account in another company where the attack can continue its path.

If cyber criminals succeed in compromising an email account used for invoicing, they can send new fake invoices containing the criminals' own account numbers, or they can change the account number in already existing invoices. If already existing email correspondence is interspersed with fake emails, it will be particularly hard for the recipient to detect the fraud without specifically checking the account numbers. One way to avoid this type of fraud is to check that the account number is correct for each payment, regardless of whether the bank involved is Danish or foreign.

Inserting phishing emails into existing email correspondence usually requires manual drafting of the fake emails. However, in 2019, organized criminals started using automated systems to send out malware embedded in thousands of phishing emails posing as answers to already existing email correspondence. The content and recipient addresses of the fake emails had been stolen in an earlier compromise.

Cyber criminals fish for company cloud email logins

More than half of all large Danish companies use office tools and emails provided as cloud solutions. The CFCS assesses that company cloud emails are the targets of a persistent cyber threat and are popular targets of phishing.

The CFCS knows of several cases in which Danish companies' cloud solutions have been the targets of compromise attempts through phishing. Cyber criminals email company employees, sending phishing emails containing a link to a false login page to the company's cloud solution.

If an employee enters their username and password at the false website, the criminals gain access to their email account that can then be used as a launch pad for further phishing activities internally in the company or against clients and sub-suppliers.

Multi-Factor Authentication (MFA) provides the best protection against this type of fraud and makes it harder, but not impossible, to carry out the fraud. One of the methods used by hackers to bypass MFA includes sending a victim to a fake login page and then transferring the username and password to the real login page. Once the MFA code is sent to the victim and the victim enters the code into the phishing page, the hackers uses the code on the real website to gain access. To avoid any suspicion, the hackers send an error message to the victim that login has failed. The method is tricky in that it must be performed before the expiry of the MFA code. Also, the method only provides one-time access to the account.

According to Microsoft 99.9 per cent of the companies whose Office365 solution has been compromised do not use MFA, and globally only a modest 11 per cent of the companies have activated MFA. The CFCS assesses that in Denmark too, many companies and private email users still have not implemented MFA login.

Most phishing activities linked to organized crime

Cyber criminals do not need to build a phishing campaign from scratch themselves. Instead, it is possible for hackers to procure all the elements needed via an underground market created and driven by organized criminals who sell or rent out their tools and infrastructure to others who want to conduct phishing attacks.

Typically, these services can be paid for anonymously in cryptocurrency, and if the hackers' phishing attacks are successful, the stolen data and accesses can be sold to other criminals.

Victim email addresses and malware are thus for sale on the Internet, and the distribution of phishing emails can take place from a so-called botnet run by other hackers. Phishing websites are easily created by use of phishing kits, and companies offering so-called bulletproof hosting make it possible for hackers to set up and run phishing websites in a way that complicates authority intervention.

Phishing kit
Creating a false website that looks and functions as a real web shop or login page is no mean feat. Catering to cyber criminals that do not have such capabilities, special forums on the Internet offer phishing kits containing all the tools and services needed to set up and run a fake website.

Criminals without hacker competencies even have the option of buying so-called phishing-as-a-service online that involves the provider running the infrastructure needed for phishing attacks.

Bulletproof hosting
Bulletproof hosting denotes hosting providers that allow criminals to rent their servers for cyber-crime purposes. Typically, they ignore enquiries by public authorities or private companies that have been scammed, making it a lengthy process to take down phishing websites hosted in this way.

Authorities in several countries are trying to close down such hosting providers. In September 2019, German police thus shut down a hosting provider operating out of a former NATO bunker that contained 200 servers with illegal websites, etc. In October 2019, the Dutch hosting provider KV Solutions was shut down. Its transgressions included allowing criminals to set up false websites on its servers.

In addition to running a criminal supply chain in support of phishing emails, organized criminal groups are also responsible for many of the phishing emails circulating.

Emotet is an example of an infamous botnet run by organized criminals. In 2019, the botnet consisted of more than 120,000 infected Internet-connected devices. Following a drop in activities over the summer of 2019, which according to security company reports resulted in a global drop in the number of registered phishing emails of almost 40 per cent, activities have picked up again, and October and November 2019 registered a total of almost 11 million phishing emails from the network.

Reports from security companies tracking devices that are part of botnets show that botnets exist in Denmark too. Some Danish telecom providers are actively working to track and purge client units infected with botnet malware, which reduce the threat from phishing and other types of cyber crime.

Functioning email addresses coveted by cyber criminals
Phishing requires access to functioning email addresses, making them, along with passwords, coveted by hackers.

Many legitimate online companies sell lists containing email addresses. They offer the buyer the opportunity to choose between country, sector, company or whether they are looking for email addresses belonging to executive staff. Such email lists are typically used in connection with marketing, but they may also be abused for phishing. Some services, such as hunter.io, offer the opportunity to search in databases with collected email addresses, facilitating searches on email addresses belonging to a certain company, etc.

Many email addresses are collected by software that scans websites, Internet forums and social media for email addresses. If the hacker wants to collect the addresses themselves, appropriate software is readily available online and can be downloaded from the Internet. As a result, email addresses that are exposed on the Internet may be particularly vulnerable to phishing and other unwanted emails.

Email addresses may also originate from companies and websites that offer a certain product or service for free, such as newsletters and reports, in return for the receiver typing in their email address to register for access.

Hackers often harvest email addresses from compromised citizens, companies or Internet services. The harvested addresses may originate from contact lists or client data. Hackers may either sell the addresses or use them in other attacks. Files containing compromised addresses are sometimes leaked on the Internet where hackers can collect and abuse them.

Leaked email addresses are abundant. The haveibeenpwned.com website contains almost 10 billion email addresses originating from data leaks. Private individuals and companies and public authorities can use the site to check if their email addresses have been exposed in a data leak. It is also possible to verify which company or Internet service is the source of the leak.

In spear phishing attacks, the hacker is ready to spend a long time probing for the targeted employee’s email address. Maybe the information is listed at the company’s website or spear phishing is sent to the main corporate email address in the hope that this will facilitate access to the target.

Hackers may also adopt a trial-and-error approach to guess the email address. Companies often use a fixed email syntax, and all the hacker needs to know is the name and email address of a random employee, gleaned, for instance, from the company’s website. From there on, it is relatively simple to guess the email address of a specific employee, who may have been selected via Linkedin. As email systems will typically return an error message to the sender if an email is addressed to a non-existing recipient, the hacker will have an easy time knowing when they have found the correct recipient address.

The above method can also be employed to find additional valid email addresses in a specific company just by using a trial-and-error approach to guessing different email addresses for the domain in question.

New phishing websites open by the thousands each day
In 2019, the Anti-Phishing Working Group (APWG) detected 65,000 new phishing websites every month on average. Many of the fake websites are created using so-called phishing kits, with hundreds of new kits being detected each year. An example in point is a phishing kit targeting Office365 that has been used against Danish companies.

As new phishing websites are mushrooming, there will always be new fake websites that are unknown to email filters and security systems and thus avoid interception.

Plethora of new top-level domains exploited for phishing
Phishing websites often impersonate legitimate websites to lure visitors into visiting them. As there are currently more than 1,500 so-called top-level domains – the website's last name if you will – fake websites may share the name of a real websites but use a different top-level domain, for instance .xyz instead of .dk. During the Covid-19 pandemic, the CFCS has thus assisted in removing the phishing website sundhedsstyrelsen.net that mimicked the Danish government website sundhedsstyrelsen.dk.

A few smaller countries such as Gabon in Africa and the Tokelau Islands, a dependent territory of New Zealand, offer free domains on their top-level domains .ga and .tk respectively. This is exploited by some cyber criminals to procure free domains for their fake websites.

Taking down fake websites may neutralize phishing emails
Most phishing emails are used in combination with a fake and malicious website. Without the website, this kind of phishing email becomes harmless. Consequently, taking down phishing websites is essential in addressing the threat from phishing.

Public authorities and private security companies are continually working to catch and take down or block phishing websites. However, criminals are equally persistent in changing the names of the false websites, moving them to servers with new IP addresses, or obfuscating the code behind the false website. Alternative countermoves include phishing websites that are only accessible for a few hours or days while the phishing campaign is ongoing. A phishing website may thus only be open for a few hours before it shuts down, only to re-open a few days later.

Hackers may also obscure the presence of a phishing website by blocking the access to the site from IP addresses and domains belonging to security companies, network scanners, search engines, etc.

Phishing websites that only exist temporarily, that change their name or IP address, or whose existence is otherwise kept secret from authorities and security companies are hard to detect and take down.

Many employees risk falling into the phishing trap
The risk of an employee opening a phishing email depends on factors such as how professional the email looks and the level of phishing awareness training the employee has received. Staff involvement in the in-house phishing email defence is thus essential to protect public authorities and private companies against phishing attacks.

Tests by IT security companies show that approximately 30 per cent of staff members who have not received awareness training will click on links in phishing emails, while the number drops to around 10 per cent post-training. Recurring training may reflect in even lower numbers, though reaching zero per cent will never be realistic.

Around 70 per cent of staff members will click on links in spear phishing emails, and emails sent from an internal email account will be perceived as legitimate by most employees.

Strong cyber defence offers protection against phishing fallout
Usually, corporate IT security depends on decisions and measures adopted by in-house IT security experts. However, when phishing emails do reach employee inboxes, the company's IT security is partially out of the hands of the in-house security experts and is instead depending on the employee choice whether or not to open a phishing email.

As email filters and awareness training are not sufficient to block all phishing emails on a daily basis, it is essential that the other in-house cyber defence measures are able to mitigate any fallout from a successful phishing attack.

A secure Domain Name System (DNS) service may thus block access to known malicious websites, while MFA can make it difficult to exploit stolen usernames and passwords, just as application whitelisting may prevent the installation of harmful software from attached files and websites.

If, despite the above measures, harmful software such as malware gets installed, anti-virus and anti-malware systems can detect and remove the malware. Finally, sound administrative procedures may prevent payouts to fraudsters on the basis of phishing emails.

If the damage is done, measures such as logging, back-ups and effective contingency plans will help limit the impact on the organization.

Recommendations

The CFCS recommends that all public authorities and private companies stay updated on the threat from phishing and include the threat in their risk assessments.

The CFCS website, cfcs.dk, has a number of guides on the phishing threat:

- Phishing – beskyt din organisation mod phishingangreb (in Danish)
- Reducér risikoen for falske e-mails (in Danish)
- Passwordvejledning (in Danish)
- Cyberforsvar der virker (in Danish)

Threat levels

The Danish Defence Intelligence Service (DDIS) uses the following threat levels.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

The DDIS applies the below scale of probability