Crime prevention on the internet

Report on the efforts of DK Hostmaster and DIFO
to prevent internet crime pertaining to IPR violations

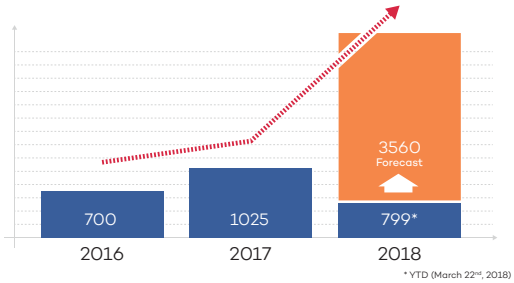
DIFO
Danish Internet Forum

Contents

Summary

At the end of 2017, DK Hostmaster implemented stricter identity checks for Danish and foreign customers. This initiative followed from a hearing on internet crime prevention hosted by DIFO/DK Hostmaster on 6 June 2016, with the participation of internet community stakeholders.

Danish customers are now required to provide proof of their identity using NemID when registering a new domain name and when accessing DK Hostmaster's self-service portal.



Foreign customers are now subject to a risk assessment when registering new domain names. If DK Hostmaster assesses the risk to be high, the customer must provide proof of their identity before obtaining authorisation to use the domain name. If DK Hostmaster assesses the risk to be low, the customer is immediately authorised to use the domain name, but must provide proof of their identity within 30 days. If DK Hostmaster assesses that there is no risk whatsoever, the customer will immediately be granted the right to use the domain name.

If the customer cannot or will not provide proof of their identity, the domain name is deleted.

DK Hostmaster also began conducting stricter identity checks of existing customers on 19 December 2017, which so far has resulted in the deletion of 2,781 domain names from the zone.

An additional 799 domain names have been seized since 1 January 2018, and 236 domain names were not registered in the zone because of failures to comply with the proof of identity requirements

› In total, 3,816 domain names have been deleted or barred from registration as a result of DK Hostmaster's intensified customer identity checks.

Significantly fewer scam webshops

Prior to the implementation of the stricter identity checks, DK Hostmaster commissioned a study which found that 3,075 webshops in the .dk zone could be suspected of being scams, corresponding to 6.74% of all web shops in the .dk zone.

Comparing this group with the group of domain names removed by DK Hostmaster in connection with the stricter identity checks and domain name seizures during the period, DK Hostmaster has eliminated domain names corresponding to 85% of the 3,075 webshops identified in the study.

The study was conducted once again after DK Hostmaster performed a risk assessment of all foreign customers, and the current findings indicate that 1.03% of all webshops are scams. The total number of scam webshops has thereby been reduced by 2,622.

					Nov. 2017	Mar. 2018
Websites suspected of intellectual property rights infringement in relation to total number active websites in local zone.	0,43%	0,25%	0,05%	0,17%	0,28%	0,04%
Web shops suspected of intellectual property rights infringement in relation to total number of web shops in local zone.	9,08%	9,52%	2,90%	6,33%	6,73%	1,03%

Source: "Analysis of Domains Suspected of Infringing Intellectual Property", conducted for DIFO by EIT DK ApS / Henrik Bjørner.
Note: Only the .dk and .se zones were examined 100% by the analysis.

› Considering the sum result of these efforts, DK Hostmaster concludes that misuse involving scam webshops has been significantly reduced, and that the .dk zone has become safer as a result.

In April-May 2018, DK Hostmaster will continue its efforts targeting existing customers. During this period, DK Hostmaster expects to identify additional customers who will be subjected to identity checks.

Background

In recent years, internet-based crime involving .dk domain names and IPR violations has increased.

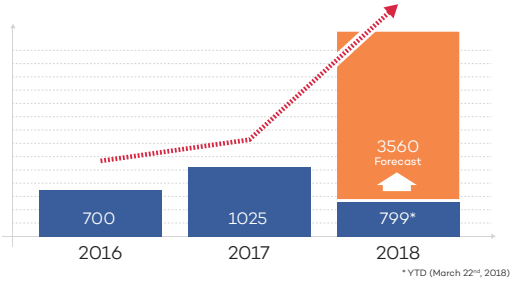
The violations occur with the creation of webshops selling counterfeit goods which appear to be goods from established brands. The product delivered is of a significantly poorer quality than the original product, and is typically an illegally manufactured counterfeit.

In other words, these webshops – also known as scam webshops – present themselves as something they are not.

The rise in this type of crime can be seen in the number of .dk domain names seized after notification of SØIK* and processing in the courts.

The figures show the trend in recent years, with actual figures until 22 March 2018.

The number of domain seizures increased from 2016 to 2018. A projection for 2018 based on year-to-date figures indicates a significant increase from 2017 to 2018.



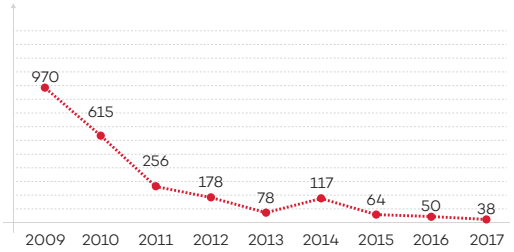
› The figures as a whole confirm that the misuse of .dk domain names is increasing.

Past misuse under .dk domain names

We have previously seen widespread misuse of .dk domain names for typosquatting, where misspellings and typos are used to generate traffic to other websites or for other criminal purposes.

In 2010, DK Hostmaster implemented a series of changes in the terms for the right of use of a domain name, whereby DK Hostmaster is now able to take action in response to complaints about potential typosquatting situations.

This power to take action has significantly diminished the problem of typosquatting, with just 38 cases reported to DK Hostmaster in 2017, compared to 970 in 2009.



The problem with IPR violations and scam webshops

As mentioned previously, the misuse of .dk domain names occurs with the creation of a webshop which is then used to sell counterfeit goods.

DK Hostmaster has analysed the domain names it has transferred to SØIK per court order as the result of a seizure. This analysis shows:

- The majority of customers are Chinese.
- Some customers have multiple domain names.
- The domain names are often ordered immediately after the domain name has become available.

DK Hostmaster's focus

DK Hostmaster does not inspect the content of websites of specific domain names. This is incompatible with DK Hostmaster's role as an infrastructure provider.

Therefore, DK Hostmaster does not view the content of websites; however, DK Hostmaster has the ability to take action and suspend or block a specific domain name if a number of conditions are not met.

**State Prosecutor for Serious Economic and International Crime*

These conditions are set forth in DK Hostmaster's terms and conditions for the right to use .dk domain names:

- In the event of typosquatting, i.e. exploiting misspellings and typos to generate traffic to other websites (Condition 9.1)
- In the event of a clear risk of economic crime, phishing, compromising of IT equipment, and/or highly offensive content combined with a risk of confusion with a third party (Condition 9.2)
- In the event of clearly illegal actions that violate significant security and public interests. (Condition 9.3)

In addition, DK Hostmaster complies with decisions and orders from Danish courts and the Complaints Board for Domain Names that require DK Hostmaster to suspend a domain name.

Stricter identity checks

Based on a June 2016 hearing of the internet community's members, the boards of directors of DIFO and DK Hostmaster decided that DK Hostmaster should implement stricter checks of who is behind a .dk domain name.

This policy change was adopted on the basis of the Danish Domain Names Act, which stipulates that DK Hostmaster is required to ensure the accuracy of the customer information behind a domain name.

Thus, DK Hostmaster now performs checks of an applicant's identity and contact information in connection with the registration of a domain name. As the technological possibilities vary greatly from country to country, the procedures for these checks are different for Danish and foreign registrations:

- The use of NemID for identity checks is required for customers with an address in Denmark. If NemID is not used, the domain name registration application is deleted.
- Customers with addresses outside of Denmark are subjected to a risk assessment. DK Hostmaster sends a request for documentation of the customer's identity if the risk is assessed as being high. The domain name is deleted if this documentation is not received within 30 days.

Efforts targeting Danish customers

On 8 November 2017, DK Hostmaster implemented mandatory use of NemID for access to DK Hostmaster's self-service portal and in connection with the registration of a domain name.

Since the introduction of mandatory NemID, 82,100 Danish customers have been validated using NemID, which provides the best possible automated identity check. This corresponds to 12.4% of all Danish customers.

As NemID is mandatory for domain name registration and the use of DK Hostmaster's self-service portal, the total number of customers validated through NemID significantly exceeds registrations during the period. (from 8 November 2017 to 21 March 2018)

Efforts targeting foreign customers

On 19 December 2017, DK Hostmaster implemented a new procedure for checking the identity of foreign customers. These procedures are rooted in the terms and conditions that also took effect that day.

Foreign customers are subjected to a risk assessment based on the information provided by the customer in the application for the domain name, the domain name itself, and the characteristics associated with the application for the domain name.

If a risk is identified, the customer is asked to provide proof of their identity. This is done with a tool also used by banks for identity verification to prevent money laundering.

If a high risk is identified, the customer must provide proof of their identity within 30 days to retain the right to the domain name. If no documentation is provided within 30 days, the domain name is deleted. The domain name is not activated in the zone until the identity of the customer has been verified.

If a low risk is identified, the domain name will be registered and activated in the zone, whereby a website can be used immediately. However, the customer must provide proof of their identity within 30 days. If this documentation is not provided, the domain name will be deleted and thereby removed from the zone.

Modern Sole Registry

DK Hostmaster is able to perform these stricter identity checks for all customers because the .dk zone is administered as a Sole Registry.

With the Sole Registry model, users are direct customers of DK Hostmaster even though the right of use of a domain name is sold through a provider. DK Hostmaster is thus able to impose requirements directly on customers.

Therefore, DK Hostmaster is also able to take action if a customer does not comply with DK Hostmaster's terms and conditions.

The alternative to a Sole Registry model is a Shared Registry, where the customer's only customer-supplier relationship is with the domain name provider. If DK Hostmaster were a Shared Registry, the establishment of a uniform procedure, e.g. identity checks, would have to be implemented by all providers, who would then have to provide an identical service for customers.

The boards of directors of DIFO and DK Hostmaster believe that a modernised Sole Registry in which providers have greater freedom to manage the customer relationship is the model that best serves customers. This ensures a balance between free and equal access to a domain name, while enabling the enforcement of principles that ensure a safe and secure .dk zone. The Sole Registry model also enables customers to freely choose between providers.

Misuse of .dk domain names for IPR violations

Prior to launching the initiatives to improve identity checks of Danish and foreign customers, DK Hostmaster commissioned an analysis of the scope of identified misuse of .dk domain names for scam webshops.

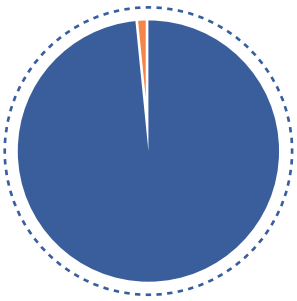
The analysis was performed by EIT DK, which under the auspices of Cybercrime.eu has conducted various analyses focusing on the misuse of domain names for IPR violations.

The analysis was performed using a web crawler, which crawls through all accessible websites in the .dk zone. When the web crawler identifies a webshop, it then examines a number of characteristics to determine whether the Webshop site appears to be genuine, and to identify indications of a scam webshop.

Based on the algorithms used by EIT DK's software to identify shops that sell counterfeit goods, the analysis found a strong suspicion that 3,075 out of the 1.33 million domain names in the Danish zone commit IPR violations.

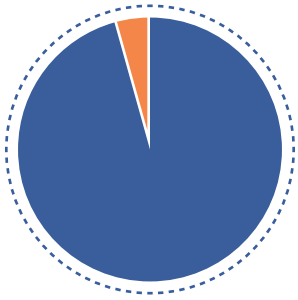
This corresponds to 0.23% of all domain names, or 0.28% of all domain names that have a website.

The total number of websites suspected of IPR violations, compared to the total number of websites



All other types of websites
1.095.019 99,72%
Suspected websites
3.075 0,28%

The total number of websites, compared to the total number of analysed websites.



Not webshops
1.052.406 95,84%
Webshops
45.688 4,16%

The same analysis indicates how many active webshops are found under .dk domain names. A total of 48,688 of the 1.33 million domain names can be identified as webshops, corresponding to 3.43% of all domain names in the zone.

The 3,075 suspected scam webshops out of the 45,688 webshops identified by the analysis indicates that 6.73% of all webshops are scam webshops.

› A suspicion that nearly 7% of all webshops identified are scams constitutes a genuine problem for the users of webshops with .dk domain names.

By comparison, here are the comparable figures for selected countries in Europe where data was available.

Websites suspected of intellectual property rights infringement in relation to total number active websites in local zone.	0,43%	0,25%	0,05%	0,17%	0,28%
Web shops suspected of intellectual property rights infringement in relation to total number of web shops in local zone.	9,08%	9,52%	2,90%	6,33%	6,73%

Source: "Analysis of Domains Suspected of Infringing Intellectual Property", conducted for DIFO by EIT DK ApS / Henrik Bjørner.
Note: Only the .dk and .se zones were examined 100% by the analysis..

Results of DK Hostmaster's efforts

DK Hostmaster's efforts have primarily involved identity checks of foreign customers.

The number of cases involving Danish customers is very low.

Foreign customers in focus

After the implementation of a risk-based model by DK Hostmaster, the following was observed:

- Many customers were categorised as high risk ("red") in the risk assessment, while a smaller number of customers were categorised as low risk ("yellow").
- After conducting the risk assessments for a period of time, the share of customers categorised as "red" has declined.

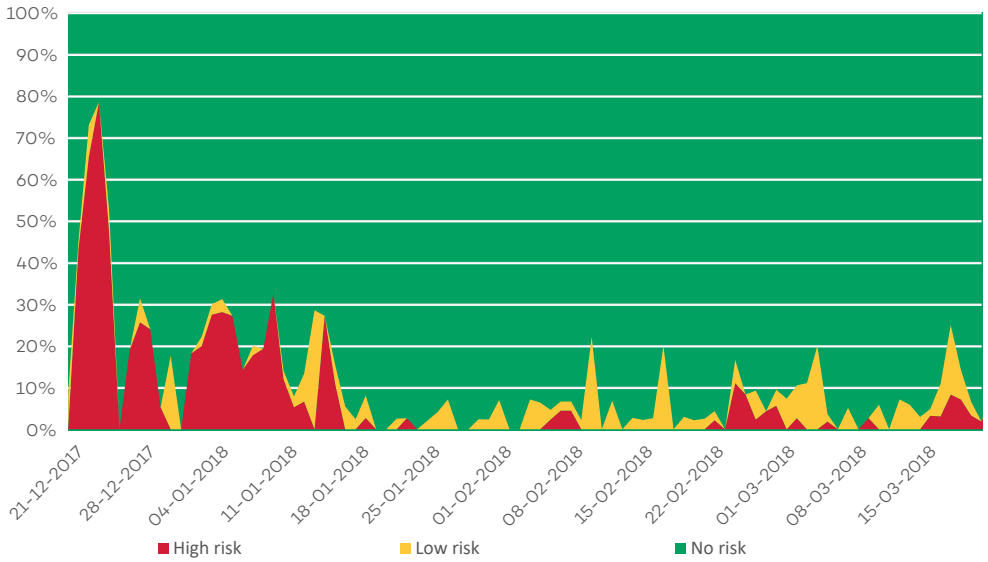
This is shown in the following figure, which presents the actual distribution of applications according to their categorisation in DK Hostmaster's risk assessment.

The figure shows that immediately after implementation of the risk assessment, DK Hostmaster found many applications to be high risk, and since then the rate has declined.

DK Hostmaster has performed a manual verification of all foreign customers who have submitted documentation and where the documentation has been approved. There are currently no indications that these domain names are being used for criminal purposes.

DK Hostmaster has also performed a manual verification of all the domain names registered by foreign customers from 20 February to 21 March 2018. There are currently no indications that these domain names are being used for criminal purposes.

Daily distribution of foreign domain applications by risk level, in percent



Overall, this indicates that DK Hostmaster's risk assessment of foreign customers has an effect.

How many submit documentation?

An important parameter in the assessment of success in limiting the establishment of new scam webshops is how the customer responds to an enquiry by DK Hostmaster asking for documentation of their identity.

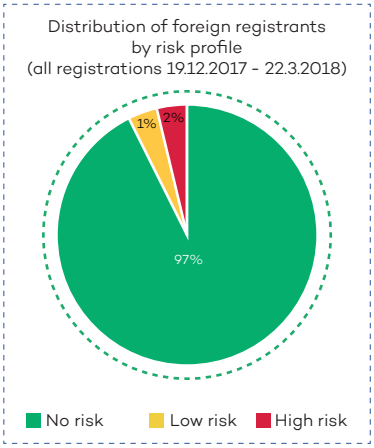
From the implementation of risk assessments until 21 March 2018, 9,880 foreign customers have been handled.

Of these, 222 were categorised as high risk and 100 as low risk.

Of the 322 customers asked to provide proof of their identity, a total of 20 have done so.

Of these 20 customers, the documentation for 15 of them was approved, and 5 were rejected.

› Thus, only a small share of those required to provide proof of their identity to DK Hostmaster in connection with an identified risk actually do so.

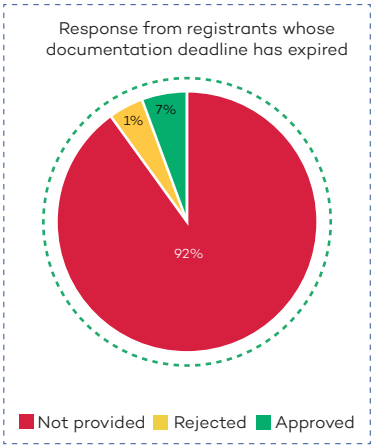


How many have been excluded from the zone?

Foreign customers are given 30 days to provide proof of their identity after a risk assessment in connection with the registration of a domain name. Looking only at foreign customers for whom the documentation period had expired by 21 March 2018, 17 out of 259 (7%) have been approved.

The domain names of the remaining 93% of customers have been deleted, either because their submitted documentation was rejected (1%) or because they did not respond to the request (92%).

› A total of 236 domain names have been deleted on this basis.



Existing foreign customers

DK Hostmaster currently has approximately 71,000 foreign customers.

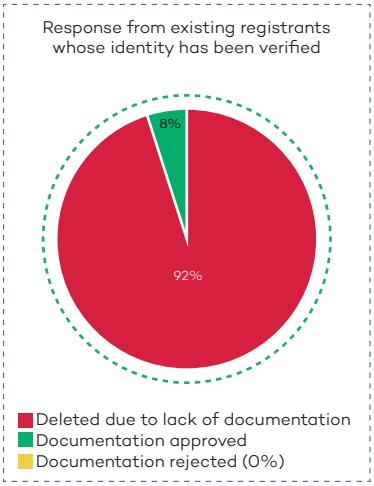
Of these existing customers, it must be assumed that a number of them possess domain names that are presently used as a platform for scam webshops.

Therefore, DK Hostmaster has subjected all existing foreign customers to an identity check.

The results found that 2,813 out of 71,000 customers were asked to provide proof of their identity. These customers own the right to use 3,395 domain names.

The domain name has been deleted in cases where the customer did not provide proof of their identity, or if the documentation was rejected. In practice, this means that the domain name is no longer active and no longer in the zone. A total of 3,124 domain names have been deleted.

Of the 2,813 customers contacted, 87 have submitted documentation. These customers have a total of 271 domain names. The documentation submitted by 84 of these customers was approved, while 3 were rejected (see figure).

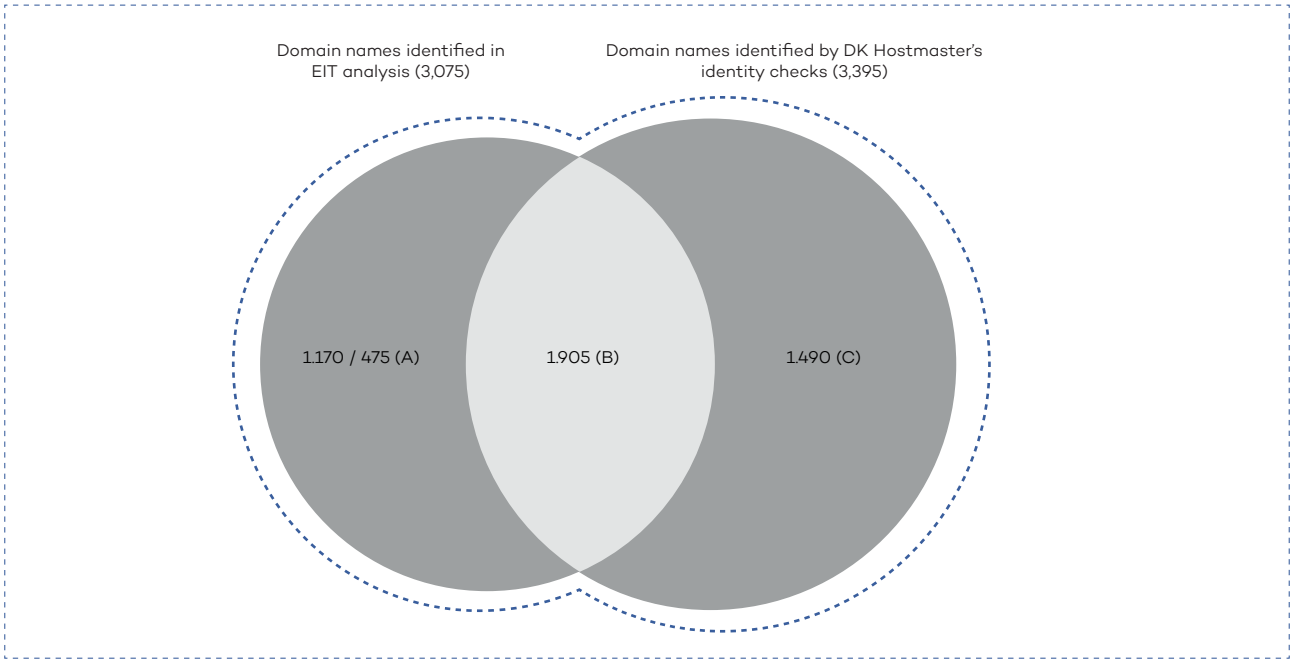


Overlap with the EIT analysis

DK Hostmaster's risk assessment of existing customers identified 2,813 customers with a total of 3,395 domain names.

As previously mentioned, prior to the implementation of mandatory use of NemID and risk assessments of foreign customers, DK Hostmaster commissioned an analysis to determine how many webshops were suspected of being scams.

It is interesting to examine the extent to which the results of the identity checks of foreign customers overlap with the results of the EIT analysis.



Group A contains domain names belonging to customers whose identity is not presently in question on the existing basis. DK Hostmaster can only remove them from the zone under court order to seize the domain name.

The EIT analysis in November 2017 found 1,170 domain names in this group. Since November 2017, several domain names have been suspended, and several of them have been seized by SØIK. Of the 1,170 identified domain names, 475 are active today.

Group B is the overlap between the two groups and comprises 1,905 domain names. In connection with DK Hostmaster's identity checks of existing customers, the domain names belonging to customers who did not successfully complete the identity check have been deleted and removed from the zone.

Group C contains the domain names belonging to customers identified in DK Hostmaster's identity check, but not in the EIT analysis. Some of these domain names were not found in the EIT analysis because they do not (yet) have an active website, and thus cannot have a potential scam webshop.
These domain names have now been deleted and are no longer available in the zone.

The above results show that DK Hostmaster is able to take action against customers who are currently operating a scam webshop – despite the fact that DK Hostmaster only acts based on information about the identity of customers.

Of the 3,075 domain names identified in the analysis, 85% have now been deleted or registered by a new customer.

› With this tool in hand, DK Hostmaster has successfully shut down many of the existing scam webshops, and given the limited number of new scam webshops open, it can be concluded that DK Hostmaster has reduced the misuse of .dk domain names for this purpose.

Current level of misuse of .dk domain names for IPR violations

To measure the concrete impact of DK Hostmaster's measures, DK Hostmaster commissioned a new analysis by EIT DK that was identical to the original analysis described previously.

The most important key figure in the analysis – the share of all active domain names that are considered to be "scam webshops" has declined from 0.28% to 0.04%.

In actual numbers, this corresponds to a drop from 3,075 to 453. As a share of all active webshops under .dk domains, the decline is from 6.7% to 1.03%.

	Websites suspected of IRP violations, as a share of total active websites in the local zone	Websites suspected of IRP violations, as a share of total webshops in the local zone
First analysis	0,28%	6,73%
Second analysis	0,04%	1,03%

› The analysis thereby confirms the strong results of DK Hostmaster's measures to limit the misuse of .dk domain names.

Overall results of DK Hostmaster's efforts

DK Hostmaster's measures have all aimed to limit the misuse of .dk domain names, improve safety and security in the zone, and maintain trust in Danish domain names.

The overall effect of implementing the new risk analysis of foreign customers on 19 December 2017 can be summarised as follows:

Number of customers asked to provide proof of identity in connection with the application for a domain name, and where they did not respond to the request or the documentation submitted was rejected.	236*
Number of deleted domain names belonging to existing customers after identity verification, and where they did not respond, or their documentation was rejected.	2.781**
Number of seized domain names under court order at the request of SØIK.	799

* 4 had submitted documentation that was rejected
** 3,124 before seizures

› In total, these initiatives have removed 3,816 domain names.

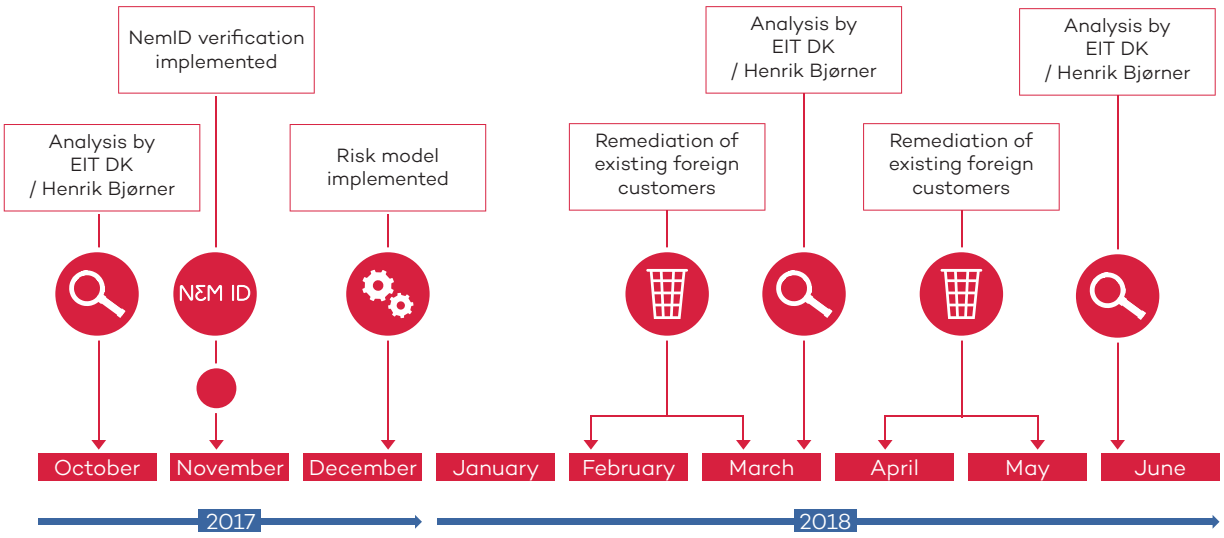
Going forward

Since the introduction of risk assessment of foreign customers in December 2017, DK Hostmaster has focused on conducting the first review of all existing foreign customers.

This has produced the results presented in the report.

During the period April – May 2018, several adjustments to the risk procedure will be implemented, and DK Hostmaster will once again analyse the existing foreign customers during this period.

DK Hostmaster expects the results of this analysis to be available in early June 2018.



Glossary of terms and concepts

This report uses a number of terms and concepts. The most important of these are explained in the following.

Customer: Used to describe the person, association or company that has the right of use of a domain name.

Provider: Used to describe DK Hostmaster's providers, who are the companies through which customers purchase their right of use of a domain name. At the time of registration, customers cannot obtain the right of use directly from DK Hostmaster, but after the first year they will typically be billed directly by DK Hostmaster.

Sole Registry: DK Hostmaster is a Sole Registry. In practice, this means that all customers have a direct customer relationship with DK Hostmaster rather than just with the provider, as is the case of a Shared Registry. This enables DK Hostmaster to impose demands directly on customers, as they are direct customers of DK Hostmaster. In a Shared Registry, this is not possible, and all regulation must be executed through the providers.

The zone: The zone comprises all accessible .dk domain names. Simply put, the zone is where a web browser looks to determine where to find a specific web address ending in .dk

Web crawler: An IT tool used to trawl through data. In this case, it is a piece of software that trawls through all .dk domain names, looking up websites and registering the characteristics of each website.

Scam webshop: A website with an webshop that is used for fraudulent purposes. For example, a site that sells counterfeit goods. These sites may also be used to collect payment information, which is subsequently used for criminal purposes.

DIFO

Danish Internet Forum

DIFO / DK Hostmaster administer domain names ending in .dk. We maintain part of the infrastructure (DNS) on the Danish part of the internet, and administer a database (WHOIS) containing master data on everyone with a registered .dk domain name.

DIFO og DK Hostmaster A/S • Ørestads Boulevard 108, 11th floor • DK-2300 Copenhagen S • www.difo.dk • www.dk-hostmaster.dk