

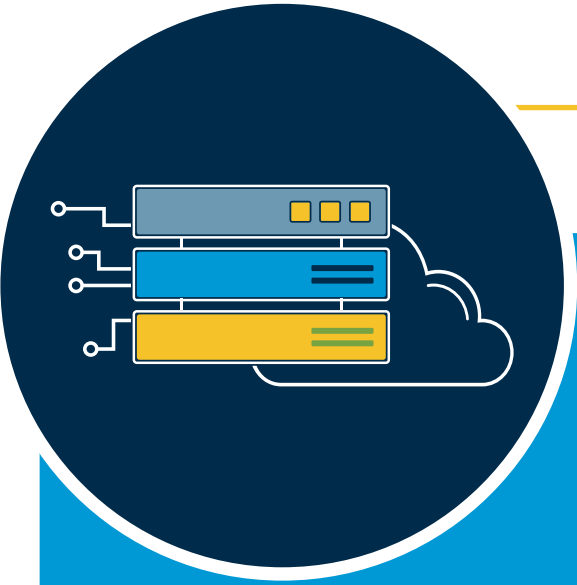


# مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات والإبلاغ عنها (DNSTICR)

يناير/كانون الثاني 2022

مؤسسة الإنترنت للأسماء والأرقام المخصصة



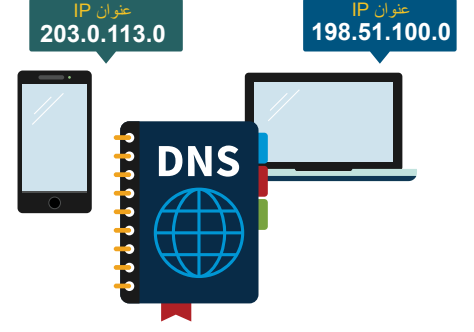


## ما الذي يتضمنه هذا الدليل؟

- 2 ما هو نظام اسم النطاق (DNS)؟
- 2 ما المقصود بتهديدات أمن نظام اسم النطاق؟
- 3 جمع معلومات التهديدات الأمنية لأسماء النطاقات والإبلاغ عنها (DNSTICR)
- 4 التهديدات غير المشمولة في نظام DNSTICR
- 5 منشأ ومصدر مشروع DNSTICR
- 6 بمقدورك المساعدة
- 7 دليل الروابط والاختصارات

## ما المقصود بنظام اسم النطاق؟

يساعد نظام اسم النطاق (DNS) المستخدمين على اكتشاف طريقهم عبر الإنترنت. فكل جهاز أو موقع ويب على الإنترنت عنوان فريد – مثل رقم الهاتف. وهذا العنوان عبارة عن سلسلة معقدة من الأرقام أو سلسلة من الأرقام والحروف يطلق عليها اسم عنوان IP. ولفظة IP هي اختصار لكلمة بروتوكول الإنترنت.



من الصعب حفظ عناوين IP في الذاكرة.  
وأن نظام اسم النطاق يجعل من السهل تصفح الإنترنت.

علمًا بأن من الصعوبة بمكان حفظ عناوين IP في الذاكرة. وأن نظام اسم النطاق يجعل من السهل تصفح الإنترنت من خلال السماح للمستخدمين بكتابة حروف معروفة - اسم النطاق - بدلاً من عنوان IP.

على سبيل المثال، يتعين عليك فقط كتابة <https://icann.org> من أجل الوصول إلى موقع ICANN على الويب، بدلاً من عنوان IP وهو -  
192.0.43.7



## ما المقصود بتهديدات أمن نظام اسم النطاق؟

هناك أشكال مختلفة للانتهاك المرتبط بالمحتوى في فضاء الإنترنت. وتشتمل بعض من هذه الانتهاكات على مواقع الويب التي توفر منصة للأنشطة غير القانونية مثل استغلال الأطفال والاتجار بالبشر. وأخرى تعمل على تعزيز التمر الإلكتروني أو عبارة عن ملاذ رقمي لبيع منتجات غير موجودة أو مزيفة.

وعلى الرغم من ذلك، فإن اختصاص ICANN لا يشمل تنظيم محتوى الإنترنت.

تركز منظمة ICANN (المؤسسة) جهودها على تهديدات أمنية محددة لنظام اسم النطاق، ذات النطاق الأضيق من الانتهاكات المرتبطة بالمحتوى. إذن، ما المقصود بتهديدات أمن نظام اسم النطاق؟

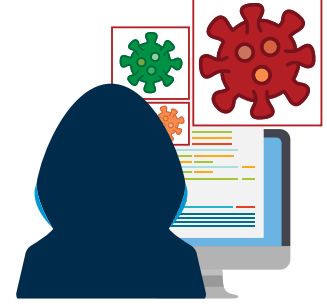
تشتمل التهديدات الأمنية لنظام اسم النطاق على أي نشاط ضار يهدف إلى إعاقة البنية التحتية لنظام اسم النطاق أو التسبب في جعل نظام اسم النطاق يعمل بطريقة غير مرغوبة.



# مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات والإبلاغ عنها (DNSTICR)

يوفر مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات والإبلاغ عنها (DNSTICR) تقارير حول تسجيلات النطاقات الحديثة التي تعتقد منظمة ICANN أنها تستخدم جائحة فيروس كورونا المستجد من أجل حملات التصيد الإلكتروني أو البرامج الضارة.

وتحتوي هذه التقارير على الأدلة التي تحدد بمنظمة ICANN للاعتقاد بأن النطاقات يجري استخدامها لأغراض خبيثة وضارة. وبالإضافة إلى المعلومات الأساسية الأخرى، تساعد التقارير أمناء السجلات المسؤولين على تقرير المسار الإجرائي الصحيح.



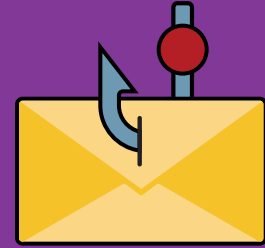
## إن مشروع DNSTICR مصمم خصيصاً للبحث عن بث البرمجيات الضارة ومحاولات التصيد.

### البرامج الضارة

هي البرمجيات التي يتم تثبيتها على أي جهاز دون موافقة من المستخدم، وتعمل على قطع أو تعطيل عمليات الجهاز أو جمع معلومات حساسة أو تتصل على وصول إلى أنظمة الكمبيوتر الخاصة. وتشمل البرمجيات الضارة كلاً من الفيروسات وبرامج التجسس وبرامج الفدية وغيرها من البرمجيات غير المرغوبة.

### التصيد والاحتيال

يحدث التصيد عندما يقوم مهاجم بخداع أحد الضحايا من أجل الكشف عن معلومات شخصية حساسة أو تخص العمل أو معلومات مالية (أرقام الحسابات أو هويات تسجيل الدخول أو كلمات مرور، إلخ)، عن طريق إرسال رسائل إلكترونية احتيالية أو مشابهة لما يريد عبر البريد الإلكتروني أو إغواء المستخدمين إلى مواقع ويب مفقدة.



# إن مشروع DNSTICR غير مخصص للبحث عن الممارسات الضارة التالية ذات الصلة بالإنترنت:

## الروبوتات

عبارة عن مجموعات من أجهزة الكمبيوتر المتصلة بالإنترنت تمت إصابتها ببرمجيات ضارة وتوجيهها إلى أداء أنشطة تحت سيطرة مدير عن بعد.



## تزوير المواقع الإلكترونية

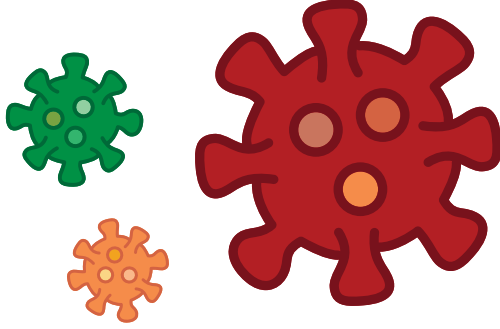
- إعادة توجيه المستخدمين إلى مواقع احتيالية أو خدمات، عادةً من خلال الاستيلاء على نظام اسم النطاق أو إفساده.
- يحدث الاستيلاء على نظام اسم النطاق عندما يستخدم المهاجمون برمجيات ضارة لإعادة توجيه الضحايا إلى موقع المهاجم بدلاً من الموقع الأصلي المطلوب.
- ويتسبب إفساد نظام اسم النطاق في جعل خادم نظام اسم النطاق أو وحدة حل التصديق إلى الاستجابة بعنوان IP مزيف يحمل شفرة ضارة. ويختلف التصيد عن تزوير المواقع الإلكترونية في أن تزوير المواقع الإلكترونية ينطوي على تعديل إدخلات نظام اسم النطاق، في حين أن التصيد يخدع المستخدمين بجعلهم يُدخلون معلومات شخصية.

## البريد غير المرغوب (حيث يستخدم في نشر التهديدات الأمنية الأخرى لنظام اسم النطاق)

بريد إلكتروني جماعي غير مرغوب، لم يمنح فيه المتلقي إنذاراً أو تصريحاً للرسالة بأن ترسل إليه وتم فيه إرسال الرسالة كجزء من مجموعة أكبر من الرسائل، وتضم جميعها بالأساس محتوى متطابقاً. ولا يمثل البريد الإلكتروني العام غير المرغوب في حد ذاته أي تهديد لنظام اسم النطاق، ولكنه قد يكون كذلك إذا كان هذا البريد الإلكتروني جزء من مخطط للتصيد.



## منشأ ومصدر مشروع DNSTICR.



أثناء جائحة فيروس كورونا المستجد، عمد المجرمون إلى تصيّد كبار السن والأطفال والمعوزين الضعفاء والغافلين. ويستهدف هؤلاء المجرمون الضحايا من جميع أنحاء العالم وبالعديد من اللغات من أجل سرقة الأموال والمعلومات الشخصية.

ويجري المجرمون والمحتالون اتصالات ويرسلون بريداً إلكترونيًا أو رسائل نصية إلى الضحايا من أجل خداعهم للكشف عن معلوماتهم الشخصية، أو شراء هويات أمصال مزيفة، أو فحوصات فيروس كورونا زائفة، أو علاجات وهمية.



وللتصديّ لأعمال التصيّد والبرمجيات الضارة على الإنترنت ذات الصلة بجائحة فيروس كورونا المستجد، قامت منظمة ICANN بتطوير مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات في ICANN والإبلاغ عنها. ويقوم هذا البرنامج بالبحث عن الأنشطة التي قد تكون ضارة لأسماء النطاقات والمعلومات الأساسية لها وإبلاغ أمناء السجلات بها. كما يوفر طبقة أخرى من الدفاع في معركة منظمة ICANN لحماية مستخدمي الإنترنت من التهديدات الأمنية لنظام اسم النطاق.



ومع استمرار الجائحة، يجري تحديث المصطلحات والمواضيع التي يتم البحث عنها عبر مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات في ICANN والإبلاغ عنها. وهذا التحديث ما هو إلا عملية فنية بسيطة نسبيًا. على سبيل المثال، تشمل المواضيع الإضافية جواز السفر، المرتبط بجوازات المناعة المستخدمة في بعض الدول، إضافة إلى أيفرمكتين، وهو عقار مضاد للطفيليات، بات مرتبطًا بالجائحة.

وقد تشتمل بعض المصطلحات الأخرى على عناوين للبرامج المدعومة من حكومات بارزة ذات صلة بجائحة فيروس كورونا المستجد تهدف إلى توفير مساعدات للمحتاجين. وهناك مصطلحات عامة أكثر مثل أجهزة التنفس الصناعي وأقنعة N95، والمعقمات مشمولة أيضًا.

وعلى الرغم من ذلك، تفتقر منظمة ICANN إلى الموارد أو التفويض اللازم للتحقق مما إن كانت جميع المواقع التي توفر هذه الإمدادات مشروعة أم لا.

# ساعدنا في حماية الإنترنت من البرمجيات الضارة ومحاولات التصيد باستغلال جائحة فيروس كورونا المستجد في موقعك.



هل أنت موفر للرعاية الصحية، أو مدير مالي، أو مشرّع حكومي، أو صانع سياسات، أو مسئول عن السلامة العامة أو متخصص في الأمن؟

## نحن بحاجة إليك!

إليك كيف يمكن العمل سويةً من أجل حماية مستخدمي الإنترنت من التهديدات الأمنية لنظام اسم النطاق:



### الخطوة 1

قم بإعداد قائمة بالكلمات بلغتك المحلية ومجموعات الحروف ذات الصلة بجائحة فيروس كورونا المستجد التي يجري استخدامها أو قد يتم استخدامها في منطقتك لاستهداف الأشخاص أو المؤسسات.

### الخطوة 2

أرسل قائمتك إلى [octo@icann.org](mailto:octo@icann.org) على أن يحتوي سطر العنوان على: **DNSTICR Term Suggestion** (أو مقترح مصطلحات برنامج DNSTICR)

To: [octo@icann.org](mailto:octo@icann.org)

Cc:

Subject: DNSTICR Term Suggestion

المصطلح 1

المصطلح 2

يجب تقديم المقترحات الجديدة بحيث يكون كل واحد في سطر داخل نص الرسالة الإلكترونية.

فعل سبيل المثال:

المصطلح 1

المصطلح 2

إذا كانت المصطلحات بحاجة لتوضيح، فأضف التوضيح بعد قائمة المصطلحات التي تقدمت بها.



# تعرف على مشروع جمع معلومات التهديدات الأمنية لأسماء النطاقات في ICANN والإبلاغ عنها (DNSTICR) وطريقة المشاركة في جعل الإنترنت مكاناً أكثر أماناً!

اعرف المزيد

زُر صفحتنا المخصصة لمشروع DNSTICR المخصصة على الويب:

<https://www.icann.org/dnsticr>



استكشف

اعرف المزيد حول الجهود المبذولة على نطاق منظمة ICANN من أجل الحد من التهديدات الأمنية لنظام اسم النطاق:

<https://www.icann.org/dnsabuse>



المختصرات والمصطلحات

انقر فوق الروابط التالية لقراءة المزيد حول الاختصارات والمصطلحات المستخدمة في هذا الدليل من خلال ميزة اختصارات ومصطلحات ICANN على:

<https://go.icann.org/acronyms>



اسم النطاق

ملصق اسم النطاق

نظام اسم النطاق (DNS)

بروتوكول الإنترنت (IP)

عنوان بروتوكول الإنترنت

بروتوكول الإنترنت الإصدار 4 (IPv4)

بروتوكول الإنترنت الإصدار 6 (IPv6)

تواصل معنا

[flickr.com/icann](https://www.flickr.com/photos/icann/)



[https://icann.org](https://www.icann.org)



[linkedin.com/company/icann](https://www.linkedin.com/company/icann/)



[icann@](mailto:icann@)



[soundcloud.com/icann](https://www.soundcloud.com/icann)



[facebook.com/icannorg](https://www.facebook.com/icannorg)



[instagram.com/icannorg](https://www.instagram.com/icannorg)



[youtube.com/icannnews](https://www.youtube.com/icannnews)



أو زُر صفحتنا المخصصة على وسائل التواصل الاجتماعي:

<https://go.icann.org/socialmedia>