

October 2024

Scam Prevention Framework Submission

Scott Morris
Regional Director
Australia and New Zealand
smorris2@infoblox.com

157 Walker Street
Level 11, Suite 1103
North Sydney, NSW 2060
AUSTRALIA

About Infoblox

Infoblox welcomes the opportunity to respond to the Scams Prevention Exposure Draft Legislation. Infoblox is the leader in next generation domain name systems management and security at scale. More than 12,000 customers, including 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. The Infoblox Cyber Intelligence Unit creates aggregates and curates information on threats to provide actionable intelligence that is high quality, timely and reliable. Infoblox Federal is a cleared US contractor supporting the US government, Five Eyes partners and public sector entities.

Executive Summary

The Scams Prevention Framework comes as the cyber security industry is experiencing major technological disruption. AI and ML-enabled cybercrime are poised to increase the scale, speed and effectiveness of internet-based scams, potentially increasing the cost to Australian consumers by orders of magnitude. Cyber solutions that detect and respond to breaches will struggle to keep pace with this new threat landscape. As the capabilities of malicious cyber actors become more effective, prevention becomes our best protection.

In the last six months Infoblox's Threat Intelligence Unit has detected a considerable increase in cyber scams targeting Australians. On 17 July 2024 Infoblox's threat analysts provided a private briefing to Australia's National Cyber Security Coordinator (NCSC) Lieutenant General Michelle McGuinness and Deputy NCSC Tony Chapman on malicious online activity disproportionately targeting Australians.

In a scam dubbed "Vigorish Viper", a sophisticated threat actor designed, developed and operated a technology suite comprising DNS, website hosting, payment mechanisms and more, and linked it to tens of seemingly unrelated gambling brands.

The heightened tempo of malicious cyber activity, such as Vigorish Viper, inevitably means an increased role for business and industry. The majority of cyber scams occur when consumers interact with what they believe is a legitimate person or entity in the mainstream digital economy but is in fact a malicious cyber actor. It is essential therefore that the SPF be robust enough to provide effective protection to consumers while at the

same time minimising the compliance burden on industry, which is already suffering under the cost of soaring cybercrime.

Infoblox believes that broad-based protective DNS capabilities offer one of the most reliable, cost-effective & scalable solutions to malicious cyber activity. An effective protective DNS capability works by identifying malicious threat actors and preventing users from accessing compromised domains.

Protective DNS provides the most effective and reliable means of blocking a device from resolving, or connecting, to a compromised domain name to an IP address on the internet. The National Security Agency estimates that protective DNS can prevent up to 92 percent of malware from accessing its payload. ([reference](#)) In practical terms this means that phishing, spear phishing, messaging and other internet-based scams are preventable once an effective protective DNS capability is in place.

Infoblox makes **four recommendations**.

1. That affected entities be required to report known compromised domains and that a list of those compromised domains be compiled by the regulator. That list can then be relayed to ISP providers, who under Section 313 (3) of the Telecommunications Act 1997 can be required to block access to those sites.
2. That entities captured under the SPF register legitimate domain particulars at a central portal to be managed by the regulator. This will allow so-called “lookalike” domains to be easily identified and subject to take-down orders.
3. That the SPF include a recommendation that affected entities captured under the SPF regime implement a protective DNS service.
4. That the SPF provides a centralised domain takedown service that enables affected entities to accelerate the takedown of domains that are used in scams.

The Scams Prevention Framework

The Scams Prevention Framework (SPF) creates a principles-based framework to protect consumers from a range of scams.

Similar to the Security of Critical Infrastructure Act, it will impose compliance obligations on the private sector, initially the telcos, the banks and digital platforms like social media, paid search engine advertising & direct messaging services.

As these sectors harden their systems and scammers move elsewhere it is expected the regime will be extended to other sectors, including the superannuation, digital currency and online marketplaces.

Infoblox supports this approach, believing that an economy-wide response to cybercrime is required, such is the scale of the threat.

The SPF is organised according to the following principles.

Prevent:

Companies will have an obligation to prevent scams through the implementation of “robust systems and procedures” across their platforms.

Infoblox agrees with this principle.

Affected entities should be required to apply appropriate controls to protect consumers of their services from all manner of scams. Providing secure multi factor authentication and end-to-end encryption of sensitive customer detail, are two common examples of consumer protections frequently employed by businesses.

Infoblox believes that companies should be accountable for the internet domains they have registered and how they are secured. Companies should monitor when so-called “[lookalike domains](#)” are registered by threat actors and actively engage a takedown service to remove those domains as soon as possible. Lookalike domains are a common tool used by cyber scammers. As AI technologies develop, these sites will become both easier to generate and harder to detect.

Companies should be required to monitor when their domains are part of or being targeted with Traffic Distribution Systems (TDS). A TDS is a difficult to detect DNS based routing mechanism employed by threat actors to guide the victim to the most effective means of compromise.

Infoblox argues that the SPF should include a requirement that companies report lookalike sites when they are detected. This will allow the regulator to compile a list of known compromised sites that can be blocked and/or taken down.

As a model for this, the drafters of the SPF should look to subsection 313(3) of Telecommunications Act [under which ISP providers can be asked to](#) block access to certain sites.

The AFP currently manages the so-called Counterfeit Goods list via this mechanism as well as the Interpol “Worst Of” list, which identifies and blocks child abuse material. Both operate under Section 313(3) of the Telecommunications Act.

Infoblox argues this represents a viable model for a future list of compromised sites.

Detect:

Companies will be required to take reasonable steps to detect scams, including as they are happening.

Infoblox agrees with this principle.

Threat intelligence providers that focus on protective DNS interrogate domain names at the time of registration and will classify them according to specific categories.

This allows for quick and effective identification of suspicious domains. For example, domains that have existed for less than 24 hours are automatically blocked by Infoblox products. This allows Infoblox’s “web crawlers” to investigate the site to see if it is legitimate or hosting illegal content or malware.

Infoblox can then determine if the domain is harmful, suspicious or legitimate and if necessary, block access.

This is a reliable and effective method of preventing scams in motion.

Report:

Infoblox agrees with this principle.

A thorough threat intelligence picture is vital to preventing internet-based scamming. Malicious threat actors are creatures of habit. They will use proven methodologies for as long as they remain effective. For a threat to be mitigated, it must first be identified.

While acknowledging the privacy and compliance issues involved in mandatory reporting regimes and urging due care and discretion in the application of any such scheme, Infoblox nonetheless believes that some kind of mandatory reporting requirement should be an element of the SPF.

By using the model of the Counterfeit Goods list and the Interpol “Worst Of” list, a reporting regime would allow for the creation of a list of known compromised sites.

Sites on this list could then be blocked using the powers described in the Telecommunications Act, under which ISP providers can be directed to block access to certain domains.

This would have a major impact on the scale and effectiveness of internet-based scams.

Disrupt:

Companies will be required to take “reasonable steps” to disrupt scams they know are in play. Those steps are likely to include “frictions/validations” to increase the chances of disrupting the scam.

Infoblox agrees with this principle.

Protective DNS when applied at an ISP level (like the Interpol and Counterfeit Goods lists) will block consumers in Australia from reaching scam sites.

A Response Policy Zone (RPZ), effectively an automated means of preventing access to certain domains, would provide real-time protection to internet users.

One of the current limitations of the Counterfeit Goods and Interpol lists is that they are updated every 24-hours.

While this is better than nothing, in the era of AI malware can proliferate or move at machine-speed, meaning considerable damage can occur in the time it takes to identify compromised sites and add them to lists.

If a block list was in place to protect consumers against scams at an ISP level, then the following responses could be initiated:

1. Businesses could report domains that are being used for scams to the AFP, enabling them to be blocked nationally.
2. A reputable Protective DNS list curated by an organisation that specialises in this area could be used as a blanket filter for compromised ISP addresses nation-wide.
3. A domain take-down order could be executed against compromised domains ensuring it would automatically be removed from DNS globally.

Respond:

This section mandates a mechanism by which consumers can report scams to companies and mandates the creation of a dispute resolution mechanism.

Infoblox is neutral on this principle.

Governance:

Companies must have documented anti-scam policies and procedures.

Infoblox agrees with this principle.

Infoblox believes that a proposed SPF should include a recommendation that affected entities include a protective DNS capability in their suite of protections.

Research from the National Anti-Scam Centre shows that scammers utilise the internet as the primary vehicle for scams. Infoblox's Threat Intelligence Unit assesses that a large percentage of scams are facilitated by traffic distribution systems (TDS) which are used by threat actors as a router for scams or malware that are incredibly difficult to detect.

Scams are also facilitated by the advertising algorithms of tech and social media companies such as Google and Facebook. Currently these companies are not obliged today to put effective protections in place.

In all of these cases the common threat vector is DNS. For a consumer to fall victim to a scam he or she must resolve one of these scam entry points to an Internet IP address.

An effective protective DNS capability rolled out at-scale is the most efficient means of preventing scams.

Proposed Legislation:

Will the proposed draft legislation achieve its objectives?

Partially. By making businesses more accountable for scams that utilise their digital infrastructure, an overall uplift in cyber standards is likely.

However, in the absence of an economy-wide protective DNS solution some scams will inevitably evade even the most stringent detection-and-response cyber solutions.

Equally, take-down services or actions are often limited by offshore factors, making the best defence blocking them.

What practical challenges will companies face in implementing the obligations?

Without tighter controls around accessibility of known bad domains in Australia companies will face difficulties in stemming the flow of scams on the wider internet affecting their customers and brand. Simply put, companies do not have control over which domains consumers have access to and what happens when they connect to the IP addresses mapped to those domains. Companies will be left to chase the latest scams rather than preventing the scams.

Use of Personal Information:

Many cyber security solutions require high volumes of personal customer information, for example credit card details or TFN, to operate. Some solutions operate by tracking the

egress of this data in flight. This exposes customer data to obvious privacy and commercial risk.

Protective DNS, however, does not rely on detecting sensitive content. Rather, it operates before customers or affected entities can interact with or resolve to compromised domains.

In that sense, protective DNS is among the least intrusive cyber mitigation strategies on offer.

Compliance Costs:

Protective DNS solutions represent one of the least expensive and least disruptive solutions to curb scams and malware in Australia, particularly when deployed at scale across the economy.

Protective DNS operates off existing DNS infrastructure. The costs of providing effective economy wide scam control lies in the provisioning of the curated response policy zone (RPZ) that integrates these systems via open standards. This RPZ can be self-generated as or obtained from reputable protective DNS threat intelligence providers such as Infoblox.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com