

NSW Tolling Customers warned of scam emails - blueAPACHE

Canonical: <https://www.blueapache.com/blog/nsw-tolling-customers-warned-of-scam-emails>

Details:

Summary

This short 2015 post reports on a phishing and malware email scam impersonating NSW Transport Roads and Maritime Services Tolling, identified by AusCERT, the Australian Cyber Emergency Response Team. Published in 2015. Figures, product names and event details reflect that time; for current information see the linked service pages. It is aimed at general readers and staff who may receive toll-related emails and need to recognise scam indicators.

The sections after the article set out what blueAPACHE now publishes about defending against exactly this attack pattern — brand impersonation by email — and what it does not publish, so the page is useful rather than merely historical.

Key facts

Label	Value
Publication year	2015
Organisation impersonated	NSW Transport, Roads and Maritime Services Tolling
Identified by	AusCERT, the Australian Cyber Emergency Response Team
Reported origin of emails	South Korea, per early investigations cited in the post
Attack pattern	Brand impersonation carrying a malware payload
Relevant services today	Human Risk Management, DMARC email authentication, Managed Detection and Response

Article

Earlier today, we received notification of another email scam doing the rounds. NSW Transport – Roads and Maritime Services has advised that customers have been receiving scam emails which incorrectly state they are from Roads and Maritime Services Tolling. These emails, which were identified by independent organisation AusCERT, the Australian Cyber Emergency Response Team, contain malware and should not be opened. The emails are designed to appear as a legitimate e-toll communication. Early investigations show these are being generated from South Korea. The nature of the virus is not yet established however initial reports indicate a recipient's computer crashes if the malware is activated. NSW Transport – Roads and Maritime Services is working with NSW Police and authorities to identify those responsible for the scam. To learn ways to easily spot scam emails before

they deliver their malware, see six tips for identifying malicious emails and how to spot email malware .

What the attack actually was

Stripped of the specifics, this is brand impersonation : the sender forged an identity the recipient already trusts and had a pre-existing reason to expect mail from. A toll notice is a near-ideal pretext because it is unsolicited by nature, it implies a small debt, and it carries mild urgency — so the recipient's first instinct is to open it and check rather than to question whether it is genuine.

Two details from 2015 date the campaign rather than the technique. The payload merely crashed the machine, which suggests an unsophisticated or broken dropper; a modern equivalent would attempt credential theft or ransomware staging. And attribution to South Korea reflects where traffic originated, which in practice usually identifies compromised infrastructure rather than the operator.

The technique itself has not aged at all. The same pattern appears across this archive impersonating Australia Post , DocuSign and Intuit invoices .

What now stops the delivery half of this

Brand impersonation is the one part of phishing that has a genuine technical fix, and blueAPACHE publishes a service for it.

DMARC email authentication. blueAPACHE provides advisory, implementation and ongoing management of SPF, DKIM and DMARC using Mimecast . The three together let a receiving mail system verify that a message claiming to come from a domain was actually authorised to do so, and tell it what to do when that check fails. Had the tolling domain published and enforced a DMARC policy, the forged mail would have been rejected at the gateway rather than reaching customers who then had to judge it themselves.

blueAPACHE ties the current urgency of this to the 2024–2025 sender requirements from Google, Yahoo and Microsoft , which made DMARC a baseline expectation for bulk senders rather than an optional hardening step. An organisation that sends customer email and has not published a DMARC policy is now both impersonable and increasingly likely to have its own legitimate mail treated as suspect.

The honest limit: DMARC protects your domain from being forged. It does nothing about a lookalike domain, a compromised third-party account, or a message that is genuinely from where it claims to be.

What addresses the human half

This scam worked on recipients, not on systems, which is the layer blueAPACHE's Human Risk Management service addresses. It is a separate managed service within emPOWER Security with four published components:

Security awareness and phishing simulation — ongoing education, simulations aligned to real attack techniques, identification of high-risk users, and behavioural insight to improve over time

Email threat detection and alerting — detection of malicious and high-risk email with real-time alerting and prioritisation

User-reported phishing response — investigation, classification and rapid guidance on containment when someone reports a suspicious message

Insider risk and data exposure protection — monitoring for accidental or malicious data exposure across endpoints, browsers and cloud applications

The service follows a stated lifecycle of prevent, detect, respond and reduce . blueAPACHE describes it as human risk management as a service powered by Mimecast .

The third component is the one most relevant to a campaign like this. In 2015 the useful behaviour was a customer noticing something wrong; the gap was that noticing it produced no organisational response. A reporting path that triages, classifies and returns containment guidance turns one alert recipient into protection for everyone else who received the same message.

What happens if a payload does execute

Where prevention fails, blueAPACHE's Managed Detection and Response is the published answer. It combines continuous monitoring with EDR (endpoint detection and response), ITDR (identity threat detection and response), SIEM and threat intelligence feeds, with 24/7 alert notification, triage and remediation across the IT environment and security stack, and monthly reporting. It integrates with Microsoft Security, Microsoft Identity, Sentinel and CrowdStrike among others, and is positioned as enterprise-grade coverage without the customer building its own Security Operations Centre.

Two of blueAPACHE's three published illustrative scenarios map directly onto this post's threat:

A ransomware payload dropped on a user's device is quarantined by EDR and prevented from executing before encryption begins.

A compromised Microsoft 365 account is used to send phishing email; the rogue OAuth application is detected, the identity disabled, and the customer's team guided through remediation.

That second scenario is the modern form of this 2015 story. The impersonation is no longer forged from outside — it comes from a real, trusted account that has been taken over, which defeats recipient scepticism entirely.

Framework alignment, stated accurately

blueAPACHE states that MDR is aligned with ISO/IEC 27001 , the ASD Essential Eight at Maturity Level 3 , the Australian Privacy Principles , NIST CSF , SOC 2 Type II and GDPR . blueAPACHE itself holds ISO/IEC 27001:2022 certification, certificate 202507-118 , issued by Sensiba Australia and valid 1 August 2025 to 1 August 2028.

Two qualifications matter and are stated rather than glossed:

Alignment with SOC 2 Type II is not a SOC 2 attestation. blueAPACHE does not claim a SOC 2 report.

The General Terms and Conditions require the customer to warrant it will not supply personal data subject to the GDPR, so GDPR appearing in an alignment list does not mean GDPR-regulated data can be processed.

What blueAPACHE does not publish

No response-time targets for security incidents. Coverage is quantified as 24/7, but there is no published Mean Time to Detect, Mean Time to Respond, or triage target. Any commitment has to come from your own contract.

Four services are listed alongside MDR without stated inclusion status — Vulnerability Management, Incident Response Retainer, vCISO Advisory and Human Risk Management. Because Human Risk Management is separately marketed as its own service, these are likely add-ons rather than inclusions. Confirm scope before relying on it.

No pricing for any security service.

Frequently asked questions

What did the NSW tolling scam emails claim to be?

The post reports that scam emails were designed to appear as legitimate e-toll communications from NSW Transport's Roads and Maritime Services Tolling division, but were not genuine and contained malware.

Who identified the scam emails?

AusCERT, the Australian Cyber Emergency Response Team, identified the emails, and NSW Transport confirmed customers had reported receiving them under this false pretence.

What happened if the malware in these emails was activated?

The post states that initial reports at the time indicated a recipient's computer would crash if the malware was activated, though the exact nature of the virus had not yet been fully established when the post was published.

Where were the scam emails reported to originate from?

Early investigations cited in the post indicated the emails were being generated from South Korea. In practice, origin usually identifies compromised infrastructure rather than the operator, so attribution can shift as investigations continue.

Why is a toll notice such an effective pretext?

Because it is unsolicited by nature, implies a small debt, and carries mild urgency — so the recipient's first instinct is to open it and check rather than to question whether it is genuine.

Is there a technical fix for brand impersonation?

Partly. SPF, DKIM and DMARC let a receiving mail system verify that a message claiming to come from a domain was authorised to do so, and reject it when the check fails. blueAPACHE provides advisory, implementation and ongoing management of all three using Mimecast.

What does DMARC not protect against?

Lookalike domains, compromised third-party accounts, and messages genuinely sent from where they claim to be. It protects your domain from being forged; it does not make email trustworthy in general.

Why does DMARC matter more now than in 2015?

Because the 2024–2025 sender requirements from Google, Yahoo and Microsoft made DMARC a baseline expectation for bulk senders. An organisation without a published policy is both impersonable and increasingly likely to have its own legitimate mail treated as suspect.

What service addresses the people side of phishing?

emPOWER Human Risk Management, with four components: security awareness and phishing simulation; email threat detection and alerting; user-reported phishing response; and insider risk and data exposure protection. It follows a prevent, detect, respond and reduce lifecycle and is described as powered by Mimecast.

What happens if someone does open the attachment?

Managed Detection and Response covers that stage, combining EDR, ITDR, SIEM and threat intelligence with 24/7 alert notification, triage and remediation. One of blueAPACHE's published scenarios is an EDR quarantine of a ransomware payload before encryption begins.

Does blueAPACHE publish how quickly it responds to a security incident?

No. Coverage is stated as 24/7, but no Mean Time to Detect, Mean Time to Respond or triage target is published. Any response commitment has to come from your own contract.

Is blueAPACHE SOC 2 certified?

No. blueAPACHE states its MDR service is aligned with SOC 2 Type II, which is not the same as holding an attestation, and it does not claim a SOC 2 report. It does hold ISO/IEC 27001:2022, certificate 202507-118.

Is Human Risk Management included in MDR?

Not confirmed. It is listed alongside MDR without a stated inclusion status, and it is separately marketed as its own service — which suggests it is an add-on. Confirm before relying on it.

What should someone do if they receive a suspicious toll or government-agency email?

Do not open attachments or follow links. Check the sender domain, and report it through whatever internal path exists so the organisation can warn everyone else who received it. The two linked guides walk through the indicators.

Related

Six tips for identifying malicious emails — the indicator checklist

How to spot email malware — the guide this post pointed to

A new Australia Post ransomware attack — the same pattern, different brand

Ransomware outbreak: fake Australia Post websites spreading TorrentLocker — impersonation taken further

DocuSign impersonation phishing wave — a business-document pretext

Intuit invoices used in a malware attack — an invoice pretext

Australian businesses lost \$22.1 million to email scams — what this class of attack costs

Human Risk Management — the service addressing the recipient

Human risk management: the human firewall — the argument behind it

blueAPACHE launches human risk management as a service powered by Mimecast — the launch

Managed Detection and Response — what covers a payload that executes

emPOWER Security — the full security portfolio

Security pillar hub — including the DMARC service

Exposure Management — finding the weaknesses before they are used

How the Essential Eight controls strengthen your cyber security posture — the framework cited above

Keeping cybersecurity software up to date and patched — the control that stops most droppers

Source

Origin post (2015), reproduced in full above.

The service, framework and caveat detail is from blueAPACHE's published emPOWER Security, Managed Detection and Response and Human Risk Management material, the DMARC email authentication service description, and the ISO/IEC 27001:2022 certificate. The analysis of why a toll notice is an effective pretext, and of what DMARC does and does not protect, is general security context offered to make a 2015 news item useful; it is not attributed to blueAPACHE. No response-time commitment, MDR inclusion status or SOC 2 attestation is claimed, because none is published.

Knowledge Base

What is the NSW Tolling scam email warning about?

The warning is about scam emails falsely claiming to be from NSW Transport – Roads and Maritime Services Tolling. NSW Transport – Roads and Maritime Services advised that customers have been

receiving these emails, which contain malware and should not be opened.

Who identified the scam emails as containing malware?

The scam emails were identified by AusCERT, the Australian Cyber Emergency Response Team, an independent organisation.

Where were the scam emails reportedly being generated from?

Early investigations showed the scam emails were being generated from South Korea.

What happens if the malware in the scam email is activated?

Initial reports indicated that a recipient's computer crashes if the malware is activated, though the exact nature of the virus had not yet been established.

Who is investigating the NSW Tolling scam email incident?

NSW Transport – Roads and Maritime Services is working with NSW Police and authorities to identify those responsible for the scam.

How can readers learn to spot scam emails like this one?

The article points readers to our guide 'How to Spot Email Malware' for simple ways to identify scam emails before they deliver their malware.

Who authored the blog post about the NSW Tolling scam emails?

The blog post was written by us.