

The biggest threat to your online security - blueAPACHE

Canonical: <https://www.blueapache.com/blog/the-biggest-threat-to-your-online-security>

Details:

Summary

This blueAPACHE post reports: A recent study by Google has found phishing to be the biggest threat to your online security. As the digital footprint of internet users expands to encompass social networks, financial records and data stored in the cloud, account takeover, or hijacking, is a widespread problem that's not just limited to high-profile accounts. It concerns Human Risk Management, emPOWER Security, Managed Detection & Response. It names Google in connection with the announcement. Published in 2017. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2017
Study	Google with the University of California, Berkeley, March 2016 to March 2017
Three market segments studied	Third-party breach credential leaks, phishing kits, keyloggers
Current-password exposure rate	25% phishing, 12% keylogger, 7% third-party breach
Relative hijack risk	Phishing victims 400 times more likely to be hijacked than a random Google user
Phishing kits identified	4,069 distinct kits
Brands spoofed	Yahoo, Hotmail, Gmail and other mail providers, generating almost 1.5 million reports; also Dropbox and Office 365
Services referenced	Human Risk Management, emPOWER Security, Managed Detection and Response
Named products or vendors	Google, PhishTrain

Article

A recent study by Google has found phishing to be the biggest threat to your online security. As the digital footprint of internet users expands to encompass social networks, financial records and data stored in the cloud, account takeover, or hijacking, is a widespread problem that's not just limited to

high-profile accounts. Often, a single account or email address underpins a user's entire online identity. Once this is compromised, a hijacker can reset a victim's passwords to other services as a stepping stone attack, download all of the victim's private data, remotely wipe the victim's data and backups or impersonate the victim to launch further attacks. In order to better understand how hijackers attempt to take over accounts in the wild, Google teamed up with the University of California, Berkeley, and using Google accounts as a case-study, analysed several black markets to see how hijackers steal passwords and other sensitive data. The study captured three market segments – 1) Credentials leaks via third party data breaches 2) Phishing kits that deceive users into submitting their credentials and 3) Keyloggers the harvest passwords from infected machines. To conduct the study, black market actors and stolen credentials were monitored using a custom developed automated framework, from March 2016 to March 2017. The result? Phishing posed the greatest threat, followed by keyloggers and finally third-party breaches. The study found that 25 percent of phishing victims have their current Google password exposed, compared to 12 percent of keylogger victims and 7 percent of victims in third party data breaches. While this is a global phenomenon, phishing largely affected victims in the United States, South Africa and Canada. Victims of phishing are also 400 times more likely to be successfully hijacked compared to a random Google user.

Phishing kits

The deadly threat stemmed from the ease of deploying phishing kits – “ready-to-deploy” packages for creating and configuring phishing content that deceive users into submitting their credentials to fake login pages – that can harvest a victim's username, password, and geolocation information among other sensitive data. The yearlong study identified 4,069 distinct phishing kits, many of which use email as a mechanism to forward stolen credentials to operators concentrated in Nigeria, the United States and other African countries. Yahoo, Hotmail, Gmail and other mail providers were the most frequently spoofed brands generating almost 1.5 million reports of stolen credentials. Other brands spoofed by the top phishing kits include file storage services like Dropbox and Office 365. What can you do? Google has reported it is using insights from the study to improve login defences for all users. It has launched new security features, including safe browsing and the Advanced Protection program to prevent attacks. Ultimately, cybersecurity is a collective responsibility and the importance of good cybersecurity hygiene cannot be overlooked. This means avoiding unfamiliar websites, never clicking on links or downloading attachments from unknown email senders, enabling multi-factor authentication (MFA), keeping systems updated with the latest security patches and using reputable security products. blueAPACHE's phishing exploit testing Software-as-a-Service (SaaS) platform, PhishTrain, is an easy way to test your employees' ability to resist such attacks. It can help you assess your staff's current security awareness level and train them to differentiate between a legitimate email and a targeted phishing email from a malicious attacker. To know more, contact the blueAPACHE security team . The original research paper can be viewed [here](#) .

Why phishing beat the other two, mechanically

The ranking, phishing then keyloggers then third-party breaches, is the study's most useful output, and the reason for the ordering is not that phishing is more common. It is that phishing yields a current, complete and immediately usable credential, and the other two do not.

Source	What the attacker gets	Why it degrades
Phishing	The password the victim typed into the fake page, at the moment they typed it, for the exact service being targeted. Many kits also capture the	It does not degrade. It is correct on arrival.

	second factor in real time.	
Keylogger	Everything typed on an infected machine, which must then be parsed to work out which string is a password for which service.	Noisy and delayed. Requires the machine to stay infected and the credential to be typed rather than autofilled.
Third-party breach	A credential from a different service, usually hashed, often years old.	Only works where the victim reused the password, and only until they changed it.

This explains the 25 / 12 / 7 per cent figures directly. Phishing produces a current password for the targeted service one in four times; a breach dump produces one only seven times in a hundred, because most of the value has already decayed.

The 400-times figure is the same point stated as risk. A phishing victim is not merely someone whose password leaked; they are someone who has demonstrated that they will enter credentials into an attacker-controlled page. That is a behavioural signal, and it predicts repeat susceptibility, which is exactly what per-user risk scoring exists to capture.

The phishing kit is the finding that matters operationally

4,069 distinct kits is the number to hold on to, because it describes an industry rather than a technique.

A phishing kit is a packaged product: the cloned login page, the credential capture script, the exfiltration mechanism, sometimes an admin panel and a victim database. It is bought, deployed to compromised hosting, and run by someone who does not need to understand how any of it works. The study found many kits forwarding stolen credentials by email to their operators, which is the tell of a commodity product sold to a non-technical buyer.

Three consequences follow, and they still hold:

The skill floor is zero. No part of running a credential-harvesting campaign requires the operator to write code. The population of capable attackers is therefore the population of people willing to buy a kit.

Quality is decoupled from the operator. A cloned Office 365 login page produced by a well-built kit is pixel-accurate regardless of who deployed it. "Look for a badly made page" stopped being advice worth giving at this point.

The real-time relay defeats one-time codes. Better kits proxy the login live: the victim enters credentials and their SMS or app code into the fake page, the kit passes both to the genuine service within the code's validity window, and the session is taken. This is why the study's own recommendation, MFA, needs a qualification the post does not make.

The MFA qualification

The post recommends enabling multi-factor authentication, which is correct. But not all second factors survive a real-time relay:

SMS codes and authenticator app codes can be relayed. The victim reads the code aloud to the attacker, in effect, by typing it into the fake page.

Push approvals can be relayed and are additionally vulnerable to fatigue, where repeated prompts eventually get approved.

Phishing-resistant factors, meaning FIDO2 security keys and passkeys, cannot be relayed, because the cryptographic assertion is bound to the genuine site's domain. A fake domain simply cannot produce a valid one.

That distinction is the single most important practical update to this 2017 post. MFA remains the right recommendation; which MFA has since become the load-bearing detail.

The stepping-stone problem

The post makes the point that a single email account underpins an entire online identity, and that a hijacker can use it to reset passwords elsewhere. In an organisational setting this generalises to something more serious than individual harm.

A compromised corporate mailbox is not just a data loss. It is:

A password reset oracle for every SaaS service that sends reset links to that address.

A trusted sender for the next campaign, which is how one compromise becomes many. Internal mail from a genuine colleague's account passes every reputation and authentication check, because it is genuine.

A persistence mechanism, through mail rules and OAuth application grants, both of which survive a password reset. This is the specific reason that resetting the password is not the same as evicting the attacker.

blueAPACHE publishes a compromised Microsoft 365 account with a rogue OAuth application attached as one of its three illustrative Managed Detection and Response scenarios, which is this exact case.

What blueAPACHE publishes now

On the product named in this post

The post names PhishTrain, a phishing simulation SaaS platform. blueAPACHE's current published offering in this space is Human Risk Management, powered by Mimecast, with four components arranged on a prevent, detect, respond and reduce lifecycle:

Awareness training on how social engineering works.

Phishing simulation, so susceptibility is measured rather than assumed.

Risk scoring, a per-user measure of susceptibility.

Targeted remediation for the users the scoring identifies.

blueAPACHE does not publish whether PhishTrain remains available, nor whether Human Risk Management succeeds it, so anyone reading this 2017 post should treat the product name as of its time and confirm the current offering directly.

The risk-scoring component is the direct answer to the study's 400-times finding. A measured per-user susceptibility score is how an organisation identifies the individuals that figure describes, before an attacker does.

Detection and response

blueAPACHE publishes Managed Detection and Response combining EDR, ITDR, SIEM and threat intelligence, operating 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike.

For credential phishing, ITDR is the decisive component. There is no malware to find; the attacker signs in with a correct password. What is observable is the authentication pattern: an unfamiliar location, an impossible travel time between two sign-ins, a new device, or a change to authentication settings.

Visibility and email authentication

blueAPACHE publishes Exposure Management as covering four visibility layers, the external attack surface layer being the one that establishes which of your mailboxes and services an attacker can enumerate.

It also publishes a DMARC capability. The precise position: DMARC stops others sending mail that claims to come from your domain. It does not stop a kit hosting a convincing copy of your login page on a domain of its own, which is what this study measured.

Services whose inclusion status blueAPACHE does not state

blueAPACHE publishes Vulnerability Management, an Incident Response Retainer, vCISO Advisory and Human Risk Management without stating whether each is included in a base engagement or priced separately.

Essential Eight and framework position

Essential Eight strategy	Relevance to credential phishing
Multi-factor authentication	The primary control, with the qualification above: phishing-resistant factors resist real-time relay, code-based and push factors do not.
Restrict administrative privileges	Determines what a hijacked account can reach. An administrative account taken by phishing is a different incident from a standard user account.
User application hardening	Reduces the browser-side paths that support credential capture.
Regular backups	Addresses the post's point about a hijacker remotely wiping data and backups.

blueAPACHE publishes alignment with Essential Eight Maturity Level 3, the highest of the three levels, alongside ISO/IEC 27001, APRA CPS 234, the NIST Cybersecurity Framework, the Australian Privacy Principles, GDPR where applicable, and SOC 2 Type II. On SOC 2, stated precisely: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one. blueAPACHE holds ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in the provision and management of its emPOWER Infrastructure and managed service offerings.

An account takeover involving personal information engages the Notifiable Data Breaches scheme under the Privacy Act 1988, which sets a 30-day window to assess a suspected eligible breach.

Contract terms

Clause 3.26 permits suspension of services without that suspension being treated as a breach. For a hijacked account this is what permits immediate isolation, which matters because mail rules and OAuth grants continue operating until they are explicitly revoked.

Clause 24.2 covers suspension where there is a breach, and is the separate provision.

What blueAPACHE does not publish

No phishing simulation baseline or target click rate , so there is no published benchmark for what an engagement is expected to achieve. Given that this post is about measured susceptibility, that is the conspicuous gap.

No statement on whether PhishTrain remains available , or on its relationship to Human Risk Management.

No mean time to detect, mean time to respond, or triage service levels. For account takeover, detection latency is measured against an attacker already inside the mailbox.

No position on which MFA methods are supported or recommended , which is the distinction that now determines whether MFA survives a modern kit.

Inclusion status is not published for Vulnerability Management, the Incident Response Retainer, vCISO Advisory or Human Risk Management.

No pricing for any security service.

Exit and transition costs are not published. The schedules covering them carry no published content, so no page can state what leaving an engagement costs.

Related

[Human Risk Management](#)

[emPOWER Security](#)

[emPOWER Security \(pillar\)](#)

[Managed Detection and Response](#)

[Exposure Management](#)

[ISO 27001 certification](#)

[Human Risk Management: the human firewall](#)

[blueAPACHE launches world-first Human Risk Management as a Service, powered by Mimecast](#)

[How to spot email malware and Cryptolocker](#)

[PayPal targeted in new phishing and malware attack](#)

[NSW tolling customers warned of scam emails](#)

[A new personalised Australia Post ransomware attack](#)

[You've invested in security, so why are breaches still happening?](#)

[blueAPACHE Security \(case study\)](#)

[Contact blueAPACHE](#)

Frequently asked questions

What organisations conducted the phishing study cited in this article, and over what period?

The article cites a study conducted by Google in partnership with the University of California, Berkeley, using Google accounts as a case study and monitoring black-market actors and stolen credentials from March 2016 to March 2017.

What percentage of phishing victims had their current Google password exposed, compared to other attack types?

The article says 25 percent of phishing victims had their current Google password exposed, compared to 12 percent of keylogger victims and 7 percent of victims of third-party data breaches.

Why did phishing rank above keyloggers and breach dumps?

Because it yields a current, complete and immediately usable credential for the exact service being targeted, and the other two do not. A keylogger produces noisy captured text that must be parsed and depends on the machine staying infected. A breach dump produces a credential from a different service, usually hashed and often years old, which only works where the password was reused and not yet changed. Phishing does not degrade: it is correct on arrival.

What does the 400-times figure actually measure?

Behaviour, not just exposure. A phishing victim has demonstrated that they will enter credentials into an attacker-controlled page, which predicts repeat susceptibility. That is precisely what per-user risk scoring exists to capture.

How many distinct phishing kits did the study identify, and where were operators concentrated?

The study identified 4,069 distinct phishing kits, many using email to forward stolen credentials to operators concentrated in Nigeria, the United States and other African countries.

Why does the number of phishing kits matter?

Because it describes an industry rather than a technique. A kit is a packaged product, the cloned page, the capture script, the exfiltration mechanism and often an admin panel, bought and deployed by someone who need not understand any of it. The skill floor is zero, and page quality is decoupled from the operator's ability, which is why "look for a badly made page" stopped being useful advice.

Does multi-factor authentication stop a phishing kit?

It depends which factor. Better kits proxy the login in real time: the victim enters their credentials and their SMS or app code into the fake page, and the kit passes both to the genuine service inside the code's validity window. SMS codes, authenticator app codes and push approvals can all be relayed this way. Phishing-resistant factors, FIDO2 security keys and passkeys, cannot, because the cryptographic assertion is bound to the genuine site's domain. That distinction is the most important update to this 2017 post.

Why is resetting the password not enough after an account takeover?

Because mail forwarding rules and OAuth application grants survive a password reset. A compromised corporate mailbox is also a password reset oracle for every service that mails reset links to it, and a trusted sender for the next campaign, since internal mail from a genuine colleague's account passes every authentication and reputation check. blueAPACHE publishes a compromised Microsoft 365 account with a rogue OAuth application attached as one of its three illustrative MDR scenarios.

What blueAPACHE product does the article recommend for testing staff resistance to phishing?

The article recommends blueAPACHE's PhishTrain, a phishing exploit testing Software-as-a-Service platform, to assess staff security awareness and train them to differentiate legitimate emails from targeted phishing attempts.

Is PhishTrain still blueAPACHE's offering?

blueAPACHE's current published offering in this space is Human Risk Management, powered by Mimecast, with awareness training, phishing simulation, per-user risk scoring and targeted remediation on a prevent, detect, respond and reduce lifecycle. blueAPACHE does not publish whether PhishTrain remains available or whether Human Risk Management succeeds it, so the product name here should be treated as of its time and the current offering confirmed directly.

Which detection capability matters most for credential phishing?

ITDR, identity threat detection and response, which blueAPACHE publishes as part of its MDR stack alongside EDR, SIEM and threat intelligence. There is no malware to find, because the attacker signs in with a correct password. What is observable is the authentication pattern: an unfamiliar location, an

impossible travel time between sign-ins, a new device, or a change to authentication settings.

Would DMARC have helped against these kits?

Not against the kits themselves. DMARC stops others sending mail that claims to come from your domain. It does not stop a kit hosting a convincing copy of your login page on a domain of its own, which is what this study measured. blueAPACHE publishes a DMARC capability, and it is valuable for the impersonation problem it does address.

Does blueAPACHE publish a benchmark for phishing susceptibility?

No. Human Risk Management includes simulation and risk scoring, but blueAPACHE publishes no baseline click rate and no target, so there is no published figure against which improvement can be measured. Given that this post is entirely about measured susceptibility, that is the conspicuous gap.

Is the information in this post still current?

No. It reports a 2017 Google/UC Berkeley phishing study and names a product of that period; for blueAPACHE's current phishing and security awareness services, see Human Risk Management and the emPOWER Security pillar page rather than this post. The study's structural findings, the ranking of credential sources and the commoditisation of phishing kits, have not dated.

Source

<https://www.blueapache.com/blog/the-biggest-threat-to-your-online-security/>

Knowledge Base

According to the Google study discussed in the blueAPACHE article, what is the biggest threat to online security?

Phishing is the biggest threat to online security, according to a study by Google, followed by keyloggers and then third-party data breaches.

What three market segments did the Google/UC Berkeley study capture regarding account hijacking?

The study captured three market segments: 1) credential leaks via third-party data breaches, 2) phishing kits that deceive users into submitting their credentials, and 3) keyloggers that harvest passwords from infected machines.

What percentage of phishing victims had their current Google password exposed, compared to keylogger and data breach victims?

25 percent of phishing victims had their current Google password exposed, compared to 12 percent of keylogger victims and 7 percent of victims in third-party data breaches.

How much more likely are phishing victims to be successfully hijacked compared to a random Google user?

Victims of phishing are 400 times more likely to be successfully hijacked compared to a random Google user.

Which countries were most affected by phishing according to the study?

Phishing largely affected victims in the United States, South Africa and Canada.

How many distinct phishing kits did the yearlong study identify, and where were operators concentrated?

The study identified 4,069 distinct phishing kits. Many of these kits use email to forward stolen credentials to operators concentrated in Nigeria, the United States, and other African countries.

Which brands were most frequently spoofed by phishing kits, and how many stolen credential reports did they generate?

Yahoo, Hotmail, Gmail and other mail providers were the most frequently spoofed brands, generating almost 1.5 million reports of stolen credentials. Other spoofed brands included file storage services like Dropbox and Office 365.

What security features has Google launched in response to insights from this phishing study?

Google has launched new security features, including Safe Browsing and the Advanced Protection program, to prevent attacks, using insights gained from the study to improve login defences for all users.

What is PhishTrain and how does it help organizations?

PhishTrain is our phishing exploit testing Software-as-a-Service (SaaS) platform. It provides an easy way to test employees' ability to resist phishing attacks, assess staff's current security awareness level, and train them to differentiate between a legitimate email and a targeted phishing email from a malicious attacker.