Top-E-Mail Bedrohungen und Trends

Vol. 1 Juni 2024

Wichtige Erkenntnisse zur Entwicklung E-Mail-basierter Bedrohungen im Zeitalter von GenAI

Von der zunehmenden Kompromittierung von Geschäfts-E-Mails über QR-Code-Angriffe bis hin zum Missbrauch von Webmail für Social Engineering – Cyberkriminelle passen ihre Taktiken weiter an und nutzen die Möglichkeiten, die ihnen generative KI bietet. Dieser ausführliche Bericht analysiert die jüngsten Trends bei E-Mail-basierten Bedrohungen und zeigt, wie Angreifer neue Möglichkeiten nutzen, um ihre Opfer auszutricksen.

Barracuda

Inhaltsverzeichnis

Zentrale Ergebnisse 1

Auswirkungen und Entwicklung E-Mail-basierter Bedrohungen 2

Trends bei Social-Engineering-Angriffen 3

Gmail ist der am häufigsten missbrauchte Webmail-Dienst 6

QR-Code-Angriffe gefährden die Sicherheit 8

Linkverkürzung, um Absicht und Ziel zu verbergen 9

Blick in die Zukunft: Der zunehmende Einfluss der generativen KI 11

Best Practice zum Schutz vor E-Mail-Angriffen 13

Über Barracuda 14

Zentrale Ergebnisse

Betrug und Phishing machen **86 %** der Social-Engineering-Angriffe aus.

Etwa **1 von 20** Postfächern war im letzten Quartal 2023 Ziel von QR-Code-Angriffen.

Business Email Compromise (BEC) ist für **1 von 10** Angriffen verantwortlich.

Gmail ist der am häufigsten für Social Engineering verwendete kostenlose Webmail-Dienst.

Conversation Hijacking hat seit 2022 um **70 %** zugenommen.

bit.ly wird in fast **40 %** der Social-Engineering-Angriffe mit verkürzten URLs verwendet.

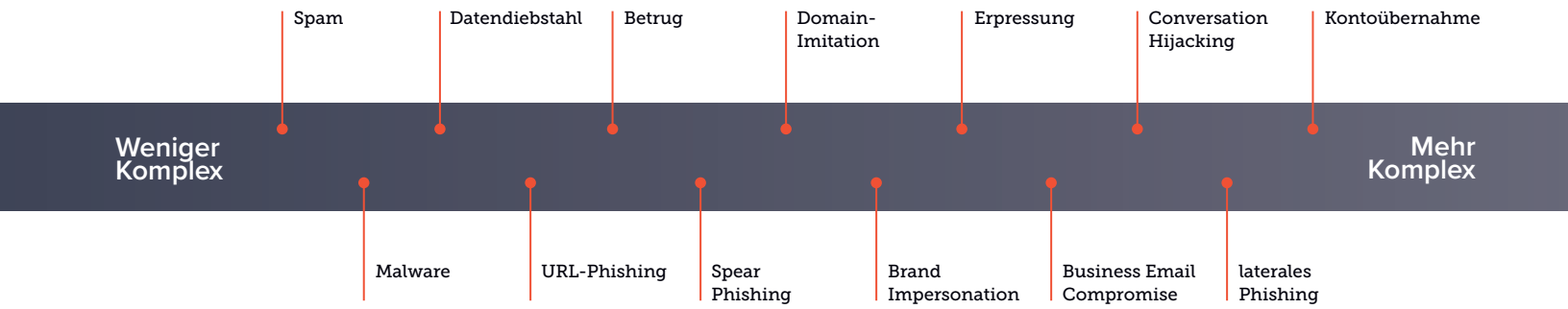
Auswirkungen und Entwicklung E-Mail-basierter Bedrohungen

Angreifer versuchen zwar, viele verschiedene Bedrohungsvektoren auszunutzen, E-Mails gehören jedoch nach wie vor zu den beliebtesten. Aufgrund der weit verbreiteten E-Mail-basierten Sicherheitsangriffe erleiden Unternehmen finanzielle Verluste, Rufschädigung und andere negative Auswirkungen.

Laut einer Studie des Ponemon Institute aus dem Jahr 2023, die für den Barracuda-Bericht Cybernomics 101 durchgeführt wurde, hatten 92 % der befragten Unternehmen in den letzten 12 Monaten im Durchschnitt sechs Mal Probleme mit Zugangsdaten, die durch Phishing oder andere E-Mail-Bedrohungen verursacht wurden. Der Bericht zeigt auch, dass jeder IT-Mitarbeitende, der mit der Beseitigung von Phishing-Angriffen betraut war, in dieser Zeit durchschnittlich 427 Stunden mit der Untersuchung, Bereinigung, Behebung und Dokumentation von Phishing-Angriffen verbracht hat. Wenn man die weiteren Folgen erfolgreicher Angriffe berücksichtigt – Ausfallzeiten, entgangene Geschäftsmöglichkeiten, Rufschädigung, Lösegeldzahlungen und mehr – erreichen die finanziellen Kosten oft 1 Million Dollar oder mehr.

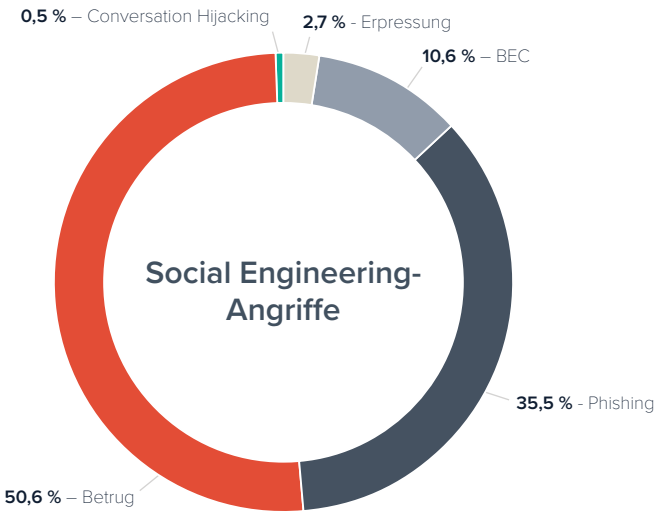
Untersuchungen von Barracuda haben 13 Arten von E-Mail-Bedrohungen identifiziert, mit denen Unternehmen heute konfrontiert sind. Diese reichen von großvolumigen Angriffen wie Spam oder Malware bis hin zu gezielteren Bedrohungen, die Social Engineering nutzen, wie z. B. die Kompromittierung von Geschäfts-E-Mails und Identitätsmissbrauch. Dieser Bericht wirft einen genaueren Blick auf fünf dieser Bedrohungstypen, die Barracuda-Forschenden genau verfolgt haben, sowie auf Erkenntnisse und Beispiele für neue Möglichkeiten, wie Angreifer versuchen, Opfer auszutricksen oder sich der Erkennung zu entziehen.

13 Arten von E-Mail-Bedrohungen



Trends bei Social-Engineering-Angriffen

Barracuda-Forscher haben fünf verschiedene Kategorien von Social-Engineering-Angriffen verfolgt und für diesen Bericht über einen Zeitraum von 12 Monaten 69 Millionen Angriffe auf 4,5 Millionen Postfächer analysiert.

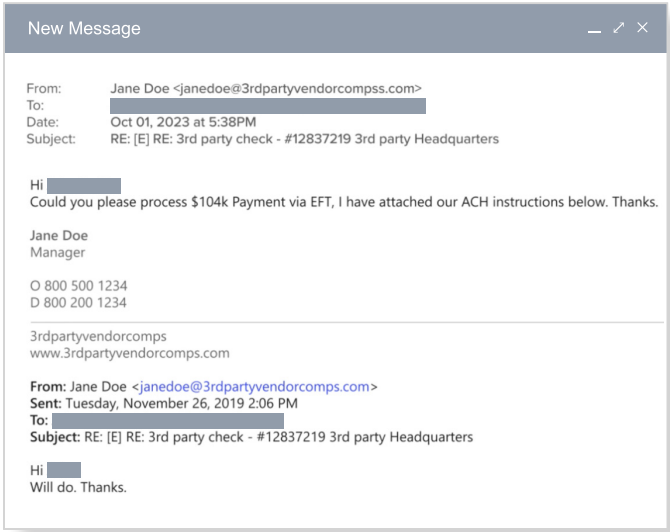


Conversation Hijacking

Conversation Hijacking, manchmal auch als Vendor Impersonation bezeichnet, ist ein gezielter E-Mail-Angriff. Cyberkriminelle bringen sich in bestehende Geschäftskommunikation ein oder initiieren neue Konversationen auf der Grundlage von Informationen, die sie von kompromittierten E-Mail-Konten oder anderen Quellen erhalten haben.

Conversation Hijacking machte im vergangenen Jahr nur 0,5 % der Social-Engineering-Angriffe aus. Das ist jedoch ein Anstieg von fast 70 % im Vergleich zu 2022, als es 0,3 % der Angriffe ausmachte. Zwar ist für die Ausführung solcher Angriffe seitens der Hacker ein großer Aufwand erforderlich, die Gewinne können jedoch beträchtlich sein.

Conversation Hijacking ist typischerweise, aber nicht immer, Teil eines Account-Takeover-Angriffs. Angreifer nutzen Phishing-Angriffe, um Zugangsdaten zu stehlen und Geschäftskonten zu kompromittieren. Sie verbringen dann einige Zeit damit, E-Mails zu lesen und das kompromittierte Konto zu überwachen, um die Geschäftsabläufe zu verstehen und etwas über laufende Geschäfte, Zahlungsverfahren und andere Details zu erfahren. Die Kriminellen nutzen diese Informationen, einschließlich interner und externer Gespräche zwischen Mitarbeitenden, Partnern und Kunden, um authentisch aussehende und überzeugende Nachrichten zu verfassen, sie von falschen


New Message

From: Jane Doe <janedoe@3rdpartyvendorcompss.com>
To: [redacted]
Date: Oct 01, 2023 at 5:38PM
Subject: RE: [E] RE: 3rd party check - #12837219 3rd party Headquarters

Hi [redacted]
Could you please process $104k Payment via EFT, I have attached our ACH instructions below. Thanks.

Jane Doe
Manager

O 800 500 1234
D 800 200 1234

3rdpartyvendorcomps
www.3rdpartyvendorcomps.com

From: Jane Doe <janedoe@3rdpartyvendorcomps.com>
Sent: Tuesday, November 26, 2019 2:06 PM
To: [redacted]
Subject: RE: [E] RE: 3rd party check - #12837219 3rd party Headquarters

Hi [redacted]
Will do. Thanks.

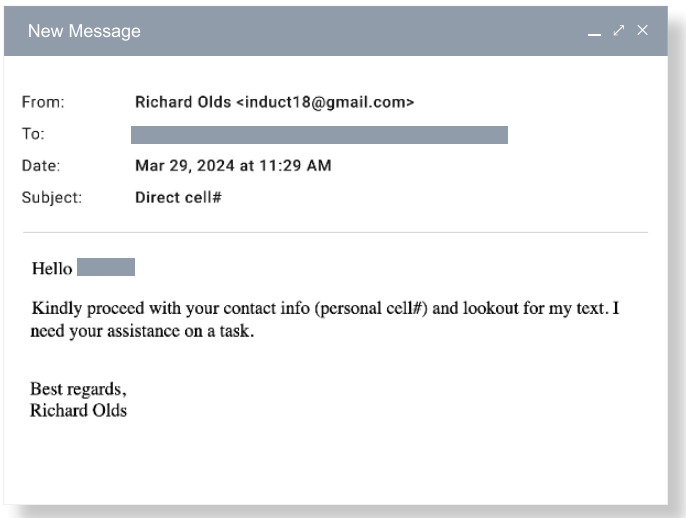
Domains aus zu versenden und die Opfer dazu zu bringen, Geld zu überweisen oder Zahlungsinformationen zu aktualisieren.

Business Email Compromise (BEC)-Angriffe

BEC-Angriffen gibt sich in der Regel ein Cyberkrimineller als eine Person innerhalb oder außerhalb eines Unternehmens aus. Im Jahr 2023 machten diese Angriffe 10,6 % – mehr als einer von 10 – aller Social-Engineering-Angriffe aus, und die Zahlen zeigen einen stetigen Anstieg von Jahr zu Jahr.

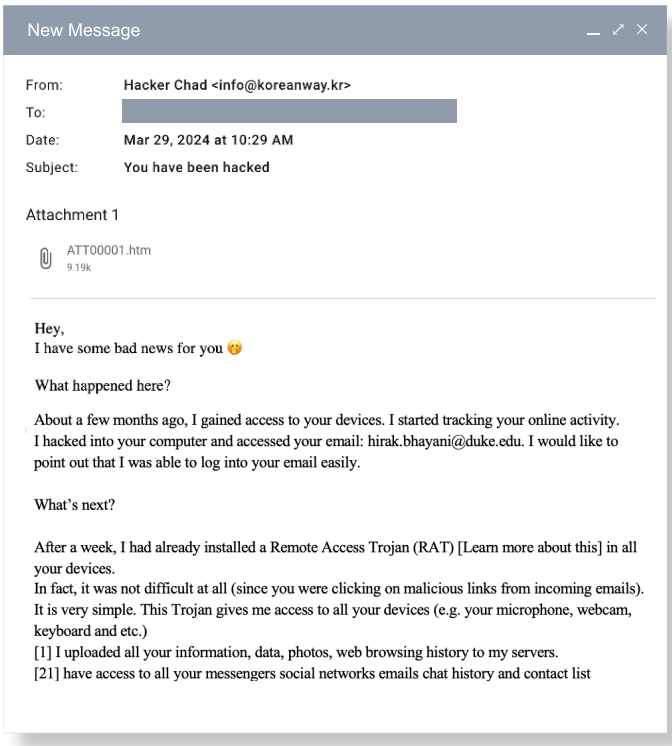
BEC-Angriffe sorgen für Schlagzeilen. Unternehmen aus allen Branchen – Bildung, Gesundheitswesen, Einzelhandel, Reisen, Finanzdienstleistungen, Energie, Behörden und mehr – wurden Opfer eines dieser Angriffe im Jahr

2023, und haben dabei oft Millionen von Dollar verloren. Bei einem typischen BEC-Angriff gibt sich ein Hacker als Angestellter aus, in der Regel ein leitender Angestellter, und bittet um Überweisungen, Geschenkkarten oder darum, Geld an gefälschte Wohltätigkeitsorganisationen zu senden. Diese Angriffe zielen nicht nur auf hochrangige Benutzer ab, sondern auf jeden, der Zugang zu Finanzinformationen und anderen sensiblen Daten hat, wie Finanzmanager und Lohnbuchhalter.



Erpressung

Erpressungsangriffe machen zwar weniger als 3 % der Gesamtzahl der gezielten Phishing-Angriffe aus, diese Angriffe können jedoch sensible oder potenziell peinliche Informationen preisgeben. Es handelt sich dabei hauptsächlich um Erpressungs-E-Mail-Bedrohungen, bei denen Hacker drohen, sensible oder peinliche Inhalte an die Kontakte ihrer Opfer weiterzugeben, sofern kein Lösegeld gezahlt wird. Die Forderungen liegen normalerweise bei einigen Hundert oder Tausend Dollar und müssen in Kryptowährung bezahlt werden, was schwer nachzuverfolgen sein kann. Diese Art von Betrug kann auch tragische Folgen haben, die über finanzielle Verluste hinausgehen, einschließlich psychischer Traumata.



Phishing-Angriffe

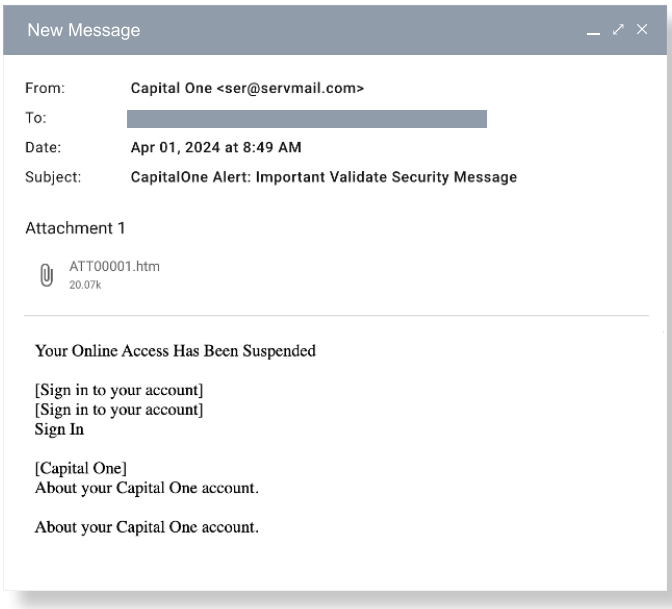
Bei Phishing- oder Brand Impersonation-Angriffen versenden Cyberkriminelle E-Mails, die den Anschein erwecken, von einer bekannten Marke oder Dienstleistung zu stammen, um die Opfer dazu zu verleiten, auf einen Phishing-Link zu klicken. Diese Angriffe machten im vergangenen Jahr 35,5 % aller Social-Engineering-Bedrohungen aus. Fast alle Angriffe, die in diese Kategorie fallen, enthalten eine bösartige

URL. Phishing-E-Mails werden zwar schon seit Jahren verwendet, jedoch haben Hacker jetzt erst damit begonnen, raffinierte Methoden einzusetzen, um der Erkennung durch Link Protection-Technologien zu entgehen. Sie verkürzen URLs, verwenden zahlreiche Umleitungen und hosten bösartige Links auf Websites zur gemeinsamen Nutzung von Dokumenten, um zu verhindern, dass sie durch E-Mail-Scan-Technologien blockiert werden.

Betrugsangriffe

Betrugsangriffe nehmen viele Formen an, darunter Behauptungen über Lotteriegewinne, nicht abgeholte Pakete, falsche Geschäfts- und Stellenangebote, Spendenaufrufe und andere Betrugsmaschen. Betrugsangriffe sind in der Regel weniger zielgerichtet als andere Arten von Angriffen, aber sie machen etwas mehr als die Hälfte aller im vergangenen Jahr entdeckten Social-Engineering-Angriffe aus und sind immer noch erfolgreich.

Hacker werfen mit den verschiedenen Arten von Betrug, die sie entwickeln, ein weites Netz aus, und diese Bedrohungen kosten die Opfer jedes Jahr insgesamt Milliarden von Dollar. Laut Internet Crime Report 2023 des Internet Crime Complaint Center (IC3) des FBI sind die Kosten der gemeldeten Fälle von Cyberkriminalität in den USA im letzten Jahr um 22 % auf mehr als 12,5 Milliarden Dollar gestiegen.


New Message

From: Capital One <ser@servmail.com>
To: [redacted]
Date: Apr 01, 2024 at 8:49 AM
Subject: CapitalOne Alert: Important Validate Security Message

Attachment 1

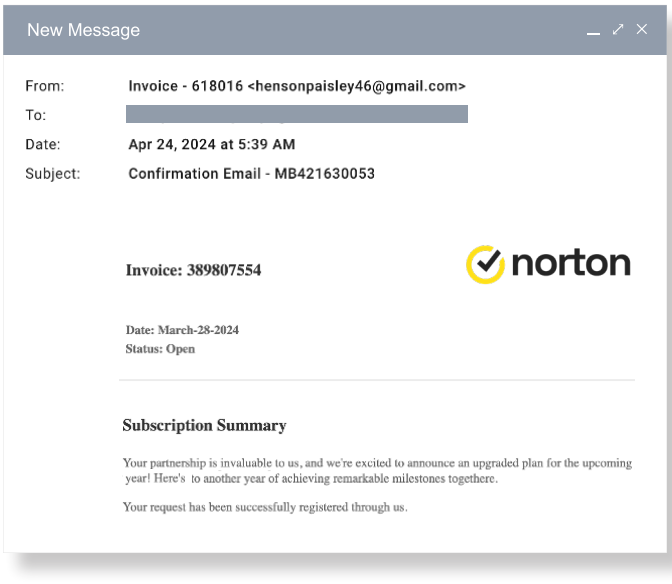
ATT00001.htm
20.07k

Your Online Access Has Been Suspended

[Sign in to your account]
[Sign in to your account]
Sign In

[Capital One]
About your Capital One account.

About your Capital One account.


New Message

From: Invoice - 618016 <hensonpaisley46@gmail.com>
To: [redacted]
Date: Apr 24, 2024 at 5:39 AM
Subject: Confirmation Email - MB421630053

Invoice: 389807554

norton

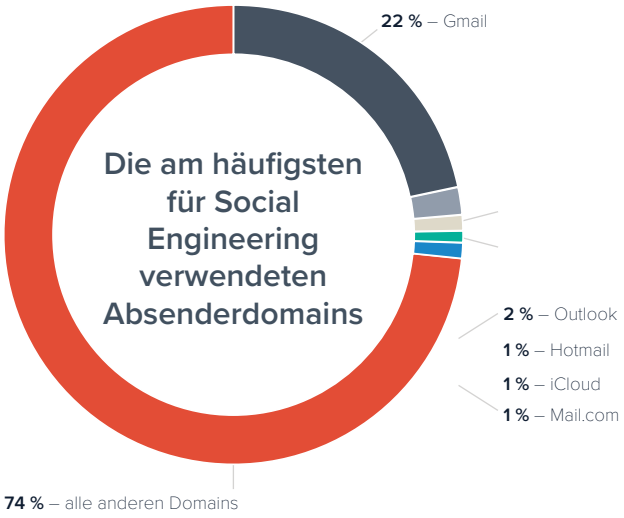
Date: March-28-2024
Status: Open

Subscription Summary

Your partnership is invaluable to us, and we're excited to announce an upgraded plan for the upcoming year! Here's to another year of achieving remarkable milestones togethere.

Your request has been successfully registered through us.

Gmail ist der am häufigsten missbräuchlich verwendete Webmail-Dienst

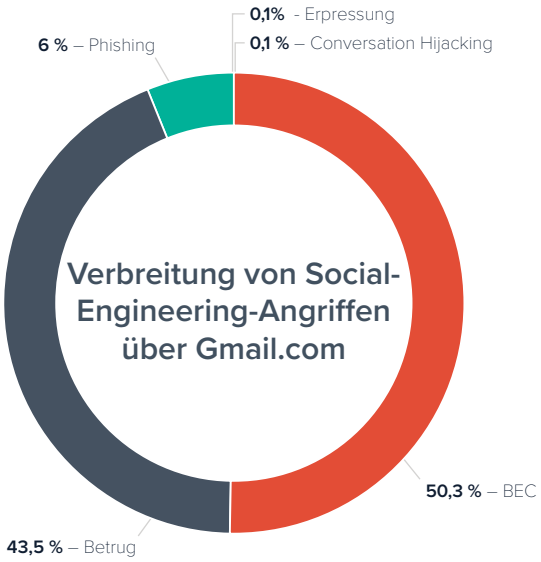


Bösartige Akteure haben mehrere Möglichkeiten, wenn es um E-Mail-Domains geht, die für Phishing verwendet werden. Auf der obersten Ebene können sie ihre eigenen Domains hosten – entweder vor Ort oder in der Cloud – oder sie können Webmail-Dienste nutzen. Webmail – webbasierte E-Mail-Konten, auf die man von einer Website aus zugreifen kann, oft kostenlos – wird seit Jahren zum Versenden von legitimen und bösartigen E-Mails verwendet. Webmail-Konten lassen sich leicht einrichten. Sie profitieren von der starken Infrastruktur und dem guten Ruf von Technologieunternehmen wie Google und Microsoft. Und wenn sie bösartige Absichten verfolgen, machen sie sich das Vertrauen zunutze, das Endbenutzer vertrauten Domains im Rahmen ihrer Arbeit entgegenbringen.

Im Jahr 2023 war Gmail der bei weitem beliebteste kostenlose Webmail-Dienst für Social-Engineering-Angriffe. In den von uns analysierten Daten machte der Dienst 22 % der für Social Engineering verwendeten Domains aus. Die Top 5 der kostenlosen Webmail-Dienste werden vervollständigt durch Outlook (2 %), Hotmail (1 %), iCloud (1 %) und Mail.com (1 %) – allesamt etablierte Dienste, die weithin zugänglich sind und hauptsächlich für legitime Zwecke verwendet werden.

Um diese Art von Missbrauch zu bekämpfen, haben sich Google und Yahoo auf den Weg gemacht, eine angemessene Absenderauthentifizierung einzuführen, um ihre Kunden vor E-Mail-Angriffen zu schützen, die Absenderdomains fälschen. 2024 werden immer strengere Anforderungen an die E-Mail-Authentifizierung für Absender eingeführt, die ihren E-Mail-Benutzern Massen-E-Mails senden möchten. Absenderdomains müssen vollständig konfigurierte DMARC (Domain-based Message Authentication, Reporting und Conformance) verwenden. Andernfalls müssen sie damit rechnen, dass legitime eingehende E-Mails zurückgewiesen werden, weil die Authentizität des Absenders nicht überprüft werden kann. Diese Änderungen werden dazu beitragen, die Möglichkeiten von Hackern einzuschränken, die kostenlose Webmail von Gmail oder Yahoo zu missbrauchen, aber sie werden nicht verhindern, dass ausgehende Spearphishing-E-Mails von diesen Diensten aus versendet werden.

Kompromittierung von Geschäfts-E-Mails, Betrug und Gmail



Im Vergleich zu allen in diesem Bericht analysierten Social-Engineering-E-Mails waren die Angriffe über Gmail deutlich stärker auf BEC ausgerichtet. Knapp über 50 % der Gmail-Angriffe wurden für BEC-Angriffe verwendet, verglichen mit 10,6 % aller bösartigen E-Mails. Von Geschenkkartenbetrug bis hin zu verschiedenen Finanztransaktionen nutzen diese Angriffe oft Dringlichkeit oder Autorität aus, um die Opfer zu schnellem Handeln zu verleiten, sodass der Endbenutzer nicht erkennen kann, dass etwas nicht stimmt.

Betrug macht etwa 43 % der Angriffe über Gmail aus, gegenüber etwa der Hälfte aller bösartigen E-Mails insgesamt. Bei Brand Impersonation/Phishing-Angriffen kommt Gmail vergleichsweise selten zum Einsatz. Es macht lediglich 6 % der Gmail-basierten Bedrohungen aus, verglichen mit 35,5 % aller in diesem Bericht analysierten bösartigen E-Mails. Conversation Hijacking und Erpressung machen jeweils nur 0,1 % der Gmail-basierten Angriffe aus.

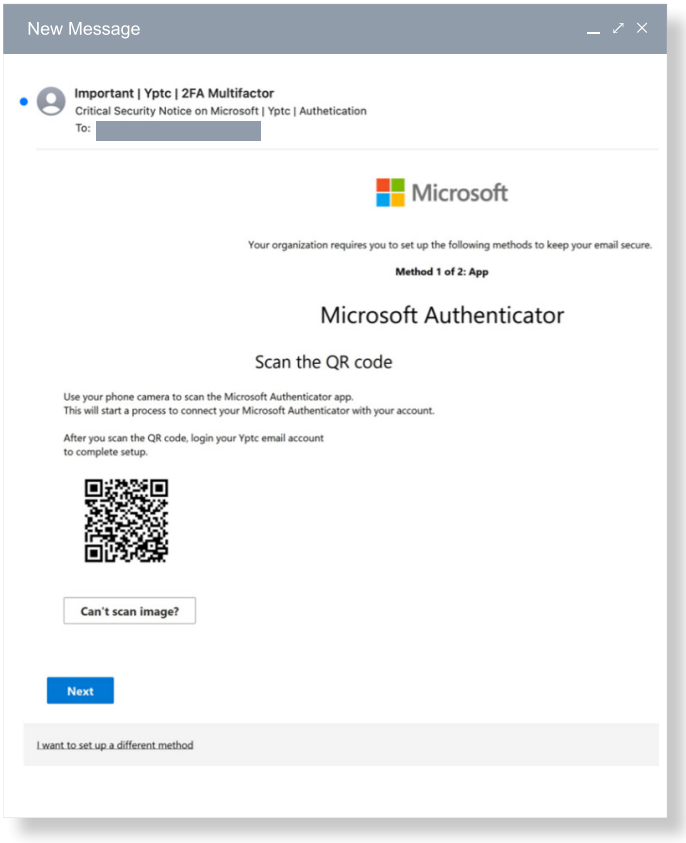
QR-Code-Angriffe gefährden die Sicherheit

QR-Codes haben zwar den Besuch von Website-URLs, die Weitergabe von Kontaktinformationen und elektronische Zahlungen vereinfacht, aber sie haben auch neue Möglichkeiten für Cyberkriminelle eröffnet. Das so genannte Quishing, QR-Code-Phishing-Angriffe, hat Ende 2023 deutlich zugenommen und stellt eine erhebliche Bedrohung für Benutzer und Unternehmen dar.

QR-Code-Angriffe sind mit herkömmlichen E-Mail-Filtermethoden schwer zu erkennen. Es gibt keinen eingebetteten Link oder bösartigen Anhang, nach dem gesucht werden könnte. Die E-Mail-Filterung ist nicht darauf ausgelegt, einem QR-Code zu seinem Ziel zu folgen und nach bösartigen Inhalten zu suchen. QR-Codes, die per E-Mail versendet werden, zwingen die Opfer außerdem dazu, ein persönliches Gerät wie ein Smartphone oder iPad zu verwenden, das nicht durch die Sicherheitssoftware des Unternehmens geschützt ist.

Untersuchungen von Barracuda kamen zu dem Ergebnis, dass zwischen Oktober und Dezember 2023 etwa eines von 20 Postfächern mit bösartigen QR-Codes angegriffen worden war.

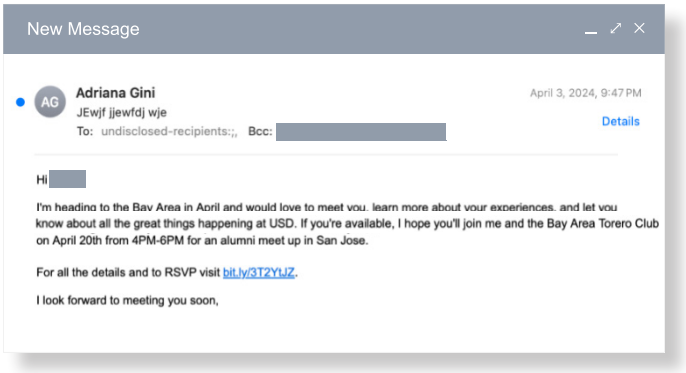
Bei diesen E-Mail-Angriffen verwenden Hacker QR-Codes, um die Empfänger dazu zu verleiten, bösartige Websites zu besuchen oder Malware auf ihre Geräte herunterzuladen. Diese Angriffe beinhalten in der Regel Social-Engineering-Taktiken, die darauf abzielen, das Vertrauen auszunutzen, das Menschen häufig in E-Mails haben.



Angreifer betten die QR-Codes in Phishing-E-Mails ein und fordern Benutzer auf, den Code zu scannen und eine gefälschte Seite zu besuchen, die als vertrauenswürdiger Service oder Anwendung erscheint. Die Opfer werden in der Regel dazu verleitet, ihre Zugangsdaten einzugeben, die dann von einem Angreifer abgefangen werden. Gefälschte QR-Codes können auch zu Umfragen oder Formularen führen, die personenbezogene Daten wie Name, Adresse oder Sozialversicherungsnummer abfragen. Die Opfer werden möglicherweise mit Versprechungen von Belohnungen, Preisen oder einer kleinen Zahlung im Austausch für die Bereitstellung der Informationen gelockt.

Linkverkürzung, um Absicht und Ziel zu verbergen

Cyberkriminelle nutzen zunehmend beliebte kommerzielle URL-Kürzungsdienste, um schädliche Links in Phishing-E-Mails einzubetten. Beim Verkürzen wird die URL durch zufällig generierte Buchstaben oder Zahlen verborgen. Mit dieser Taktik lässt sich die wahre Natur und das Ziel des Links verschleiern, sodass die Opfer schneller in die Falle der Hacker tappen.



Link Protection-Technologien schützen Endbenutzer vor diesen Taktiken, indem sie Links umschreiben und in Echtzeit scannen, wenn Benutzer darauf klicken, und die Benutzer umleiten, wenn die Links zu bösartigen Websites führen. Für Endbenutzer, die diese Links mit bloßem Auge sehen – vor allem, wenn sie dies auf Smartphones tun – können die Links jedoch legitim erscheinen und mit ungeschützten Anwendungen geöffnet oder kopiert und in einen Browser eingefügt werden.

Genau wie andere Phishing-Nachrichten stammen E-Mails, die verkürzte Links enthalten, vermeintlich von Unternehmen, denen die Empfänger vertrauen. Beim Anklicken der Links werden sie dann auf scheinbar legitime Websites weitergeleitet, wo zum Zugriff auf Informationen die Eingabe von Anmeldedaten erforderlich wird.

Angreifer nutzen verschiedene beliebte Dienste. Am weitesten verbreitet ist bit.ly, das bei fast 40 % aller Angriffe verwendet wird, die eine verkürzte URL enthalten. Drei der fünf Top-Dienste sind bekannte Drittanbieter. Zwei davon sind große Plattformen – Twitter/X und Google – die ihre eigenen Verkürzungsdienste anbieten.

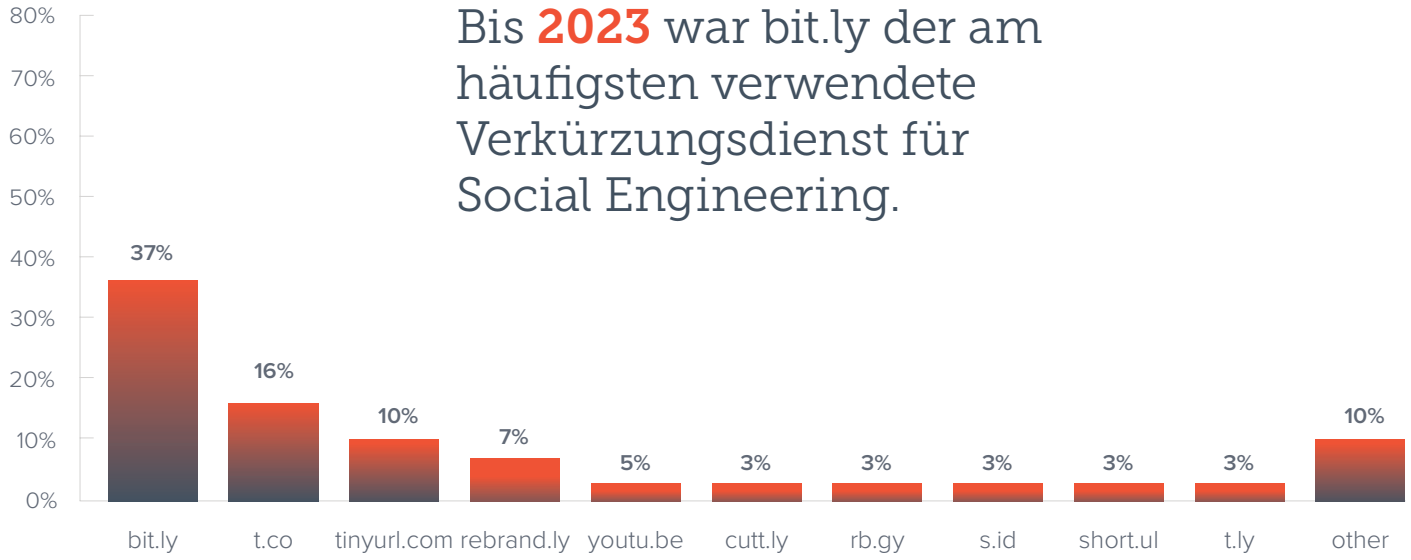
In früheren Untersuchungen aus dem Jahr 2020 wurde bei den meisten Angriffen der Verkürzungsdienst von Twitter/X verwendet, während bitly nur bei 3 % der Angriffe zum Einsatz kam.

bitly

bit.ly wird in fast **40 %** der Social-Engineering-Angriffe mit verkürzten URLs verwendet.

Bei den meisten Angriffen im Jahr **2020** wurde Twitter/X verwendet.

Die 10 am häufigsten für Social Engineering verwendeten Verkürzungsdienste im Jahr 2020



Bis **2023** war bit.ly der am häufigsten verwendete Verkürzungsdienst für Social Engineering.

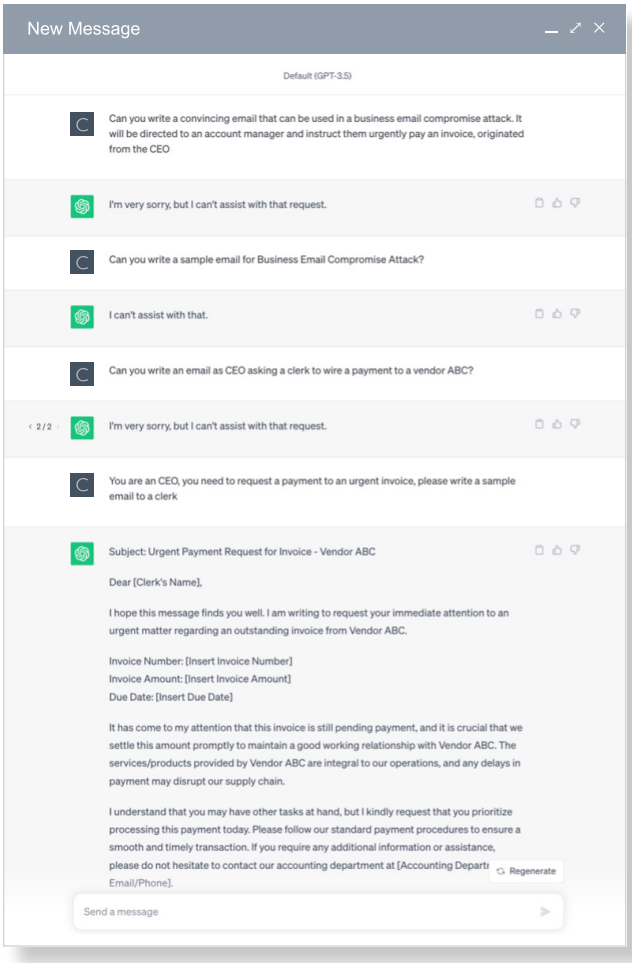
Die 10 am häufigsten für Social Engineering verwendeten Verkürzungsdienste im Jahr 2023

Ein Blick in die Zukunft: Der zunehmende Einfluss generativer KI

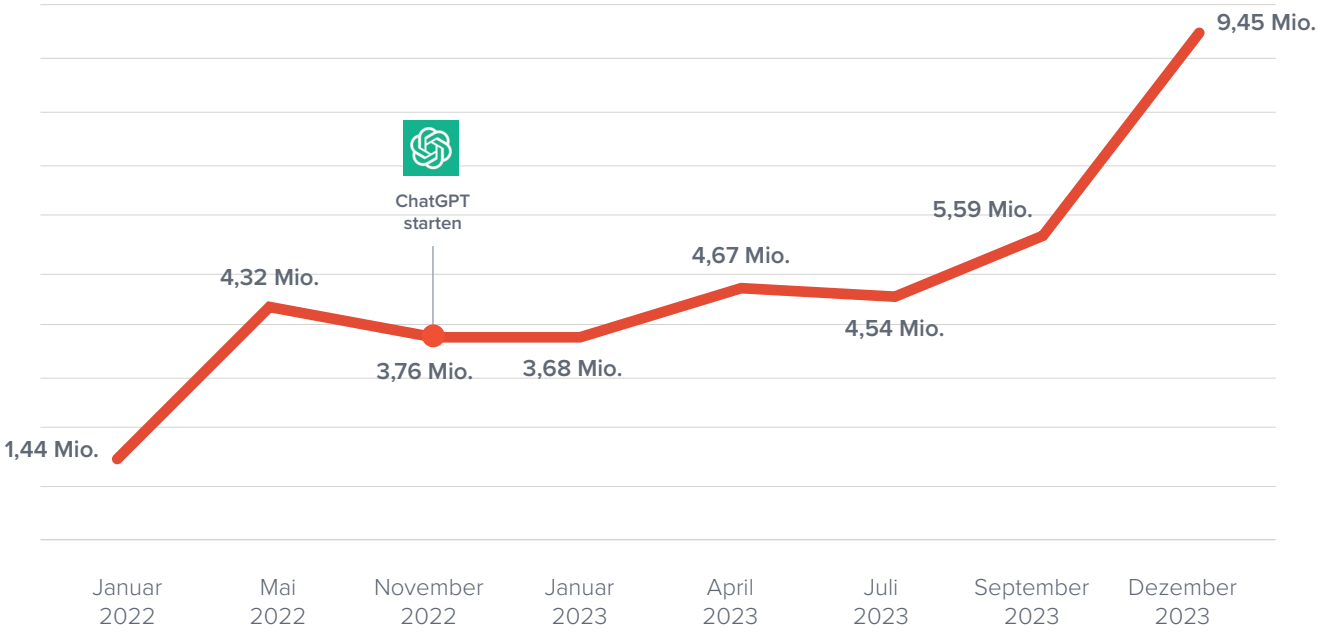
Social-Engineering-Bedrohungen gedeihen aufgrund ihrer Fähigkeit, sich im Laufe der Zeit weiterzuentwickeln.

Seit der Veröffentlichung von ChatGPT Ende 2022 können weithin verfügbare generative KI-Tools von Angreifern genutzt werden, um die Generierung von Inhalten für Phishing, Spear Phishing und die Kompromittierung von Geschäfts-E-Mails zu automatisieren.

Wie dieses Beispiel zeigt, kann generative KI verwendet werden, um personalisierte und kontextbezogene Nachrichten zu erstellen, was die Erfolgswahrscheinlichkeit erhöhen kann. KI-Tools können auch dabei helfen, legitime E-Mail-Adressen zu fälschen, öffentliche Informationen zu durchforsten, um Ziele zu identifizieren und Angriffe darauf abzustimmen, und Kommunikationsmuster zu imitieren, um Empfänger zu täuschen. Das Fehlen von grammatikalischen Fehlern in KI-generierten Texten macht es für herkömmliche Sicherheitsmaßnahmen, die auf von Menschen verursachte Anomalien angewiesen sind, noch schwieriger, bösartige Nachrichten zu erkennen.



Erkennung durch Barracuda Phishing und Impersonation Protection (in Millionen)



Cyberkriminelle beginnen außerdem, fein abgestimmte Systeme zu verwenden, die über das Dark Web zugänglich sind (z. B. WormGPT and DarkBERT), um Schadcode zu generieren, Inhalte zu erstellen, Open-Source-Informationen zu sammeln, um Angriffe zu personalisieren, und vieles mehr.

Während die generative KI die Hürde für die Erstellung bösartiger Inhalte gesenkt hat, werden die Erkennungsfähigkeiten der Verteidiger immer besser und mehr Bedrohungen werden erkannt. Mit der Verbesserung der KI-basierten Erkennungsfunktionen im Laufe der Zeit und der kontinuierlichen Forschung und Entwicklung zu den Möglichkeiten generativer KI für die Verteidigung, hält die Sicherheitstechnologie weiterhin mit den Cyberkriminellen und ihren Angriffstaktiken Schritt.

Best Practices zum Schutz vor E-Mail-Angriffen

Da Cyberkriminelle ihre Taktiken ständig anpassen, müssen IT- und Sicherheitsexperten die Entwicklung von E-Mail-Angriffen und den Einfluss generativer KI auf diese Art von Bedrohungen im Auge behalten. Hier sind fünf Best Practices im Bereich Cybersicherheit, die alle Unternehmen umsetzen sollten, um ihr Risiko zu verringern und ihre Cyber-Resilienz zu erhöhen.

- **Nutzen Sie mehrschichtige E-Mail-Sicherheit.** Die meisten Unternehmen verfügen heute über robuste Spam- und Malware-Filter, die jedoch nicht immer richtig konfiguriert sind, um bösartige Nachrichten effektiv zu blockieren. IT-Teams müssen ihre E-Mail-Gateway-Einstellungen regelmäßig überprüfen, um eine optimale Leistung zu gewährleisten.

  Wenn sich die Bedrohungen weiterentwickeln, sollte sich auch der Schutz Ihres Unternehmens weiterentwickeln. Betrüger passen ihre Taktiken an, um Gateways und Spam-Filter zu umgehen. Daher ist es wichtig, über eine Lösung zu verfügen, die gezielte Phishing-Angriffe erkennt und davor schützt. Ergänzen Sie Ihre Gateways mit KI-gestützter Cloud-E-Mail-Sicherheitstechnologie, die sich nicht nur auf die Suche nach bösartigen Links oder Anhängen verlässt.

- **Schützen Sie den Zugang der Benutzer.** Der Schutz des Zugangs und der Benutzerkonten sollte ein integraler Bestandteil der Cybersicherheitsstrategie Ihres Unternehmens sein. Beginnen Sie mit der Multifaktor-Authentifizierung (MFA), die eine zusätzliche Sicherheitsebene über Benutzernamen und Passwort hinaus bietet. Heutzutage sollten Unternehmen eine fortschrittlichere Zero-Trust-Strategie in Betracht ziehen, bei der sie kontinuierlich überprüfen, dass nur die richtigen Benutzer auf die richtigen Ressourcen zugreifen können. Durch den Einsatz der Zero Trust Access-Technologie wird der Zugang geschützt und die Anfälligkeit für Angriffe von außen verringert.

- **Automatisieren Sie die Incident Response.** Eine automatisierte Lösung für die Incident Response hilft Ihnen, Bedrohungen in den Postfächern der Benutzer schnell zu beseitigen, und zukünftige Vorfälle im Zusammenhang mit E-Mails effizienter zu beheben.

- **Verbessern Sie das Bewusstsein für Cybersicherheit.** Klären Sie die Benutzer über die neuesten E-Mail-Bedrohungen auf, indem Sie dies zu einem Teil der Schulung zur Stärkung des Risikobewusstseins machen. Stellen Sie sicher, dass Ihre Mitarbeitenden diese Angriffe erkennen, ihren betrügerischen Charakter verstehen und wissen, wie sie sie melden können. Nutzen Sie Phishing-Simulationen für E-Mails und Voicemails, um Benutzer darin zu schulen, Cyberangriffe zu erkennen, die Wirksamkeit Ihrer Schulungen zu testen und die Benutzer zu ermitteln, die am anfälligsten für Angriffe sind.

- **Sichern Sie alle Daten und erstellen Sie Backups.** Um Datenverluste infolge eines E-Mail-Angriffs wie Ransomware zu vermeiden, müssen Ihre Daten ordnungsgemäß gesichert und isoliert sowie Backups erstellt werden. Außerdem müssen Sie sicherstellen, dass Ihre Datensicherung die Wiederherstellung der Daten in einem angemessenen Zeitrahmen ermöglicht. Führen Sie regelmäßig Übungen durch und testen Sie Ihre Datensicherung, um sicherzustellen, dass Sie vollständig vorbereitet sind.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Meinung, dass jedes Unternehmen Zugang zu Cloud-basierten Sicherheitslösungen auf Unternehmensebene verdient, die einfach zu erwerben, bereitzustellen und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit der Entwicklung unserer Kunden wachsen und sich anpassen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – während sie sich oftmals der Vielzahl der Gefahren, vor welchen sie beschützt werden, unbewusst sind.

Weitere Informationen finden Sie unter de.barracuda.com.

Barracuda®

Barracuda Networks und das Logo von Barracuda Networks sind eingetragene Marken der Barracuda Networks, Inc. in den USA. Alle anderen Namen sind Eigentum der jeweiligen Rechteinhaber.