Mit welchen Maschen Internetbetrüger Ihr Unternehmen angreifen

Unsere Liste der 10 häufigsten Cyberbetrugsmethoden

Cyberangriffe sind ein gewaltiges Problem. Durch sie haben Unternehmen allein im vergangenen Jahr weltweit sage und schreibe 9 Billionen EUR verloren. Und Unternehmen aller Größen sind davon betroffen.

In diesem Guide werden Sie von uns erfahren, welche 10 Maschen die Internetbetrüger von heute am häufigsten verwenden und wie Sie sich und Ihr Unternehmen vor ihnen schützen können.

brother
at your side

Mehr als die Hälfte aller Cyberangriffe richten sich gegen KMUs

60 % der Unternehmen dieser Größenordnung müssen innerhalb von 6 Monaten nach einem erfolgreichen Hackerangriff ihre Geschäftstätigkeiten einstellen* – eine schockierende Zahl.

Und selbst wenn Firmen einen solchen Angriff überleben, haben sie oft lange unter den enormen Folgeschäden zu leiden – von erheblichen finanziellen Verlusten bis hin zur Rufschädigung durch Ransomware.

Um Sie vor diesen gravierenden Folgen zu schützen, haben wir für Sie die zehn am häufigsten verwendeten Cyberbetrugsmethoden zusammengestellt – nebst Tipps, wie Sie sich dagegen wappnen können.

Laut einer jüngsten Umfrage von Brother fühlen sich viele IT-Entscheidungsträger nicht gut genug für die Abwehr der häufigsten Arten von Cyberangriffen vorbereitet, allen voran Malware, Ransomware und Phishing.

Außerdem finden es viele von ihnen schwierig, ihr IT-System dauerhaft vor solchen Angriffen zu schützen.

44 % der IT-Entscheider betrachten das Management dieser Systeme sogar als ihre größte Herausforderung.

Deshalb sind wir von Brother auch hier wieder „At your side“, um Sie bei der Abwehr von Cyberangriffen zu unterstützen.

Sicher ist es nicht immer leicht, die praktischen Informationen zu finden, die Sie dafür brauchen, um zu wissen, wo die Gefahren lauern und wie man sie frühzeitig erkennt und sich umfassend vor ihnen schützt.

Deshalb haben wir für Sie einige der typischsten und effektivsten Betrugsmethoden zusammengestellt, auf die Sie vorbereitet sein sollten. Und damit Sie sich rundum schützen können, ohne Ihr Tempo drosseln zu müssen, geben wir Ihnen noch einige nützliche Tools und Informationen zur effizienten Gefahrenabwehr mit auf den Weg.

Lernen Sie nun die 10 häufigsten Cyberbetrugsmaschen kennen, um Online-Betrügern nicht auf den Leim zu gehen.

*TechRound März 2023

Wussten Sie’s schon?

Die am häufigsten zum Phishing missbrauchten Marken sind Microsoft (29 %), Google (13 %) und Amazon (13%).

Die Betrugsmasche

Ein Mitarbeiter erhält eine Nachricht – in der Regel eine E-Mail –, die von einem vertrauenswürdigen Unternehmen wie Apple oder Google zu kommen scheint. Sie könnte sogar über Microsoft Teams verschickt worden sein.

Wie bei vielen anderen Arten des Internetbetrugs könnte der Absender behaupten, es sei DRINGEND nötig, SOFORT etwas Bestimmtes zu tun, wie etwa, auf einer Website Kontodaten, Zahlungsinformationen oder Passwörter einzugeben.

Dabei bedienen sich Online-Betrüger leider oft sehr bekannter Marken wie Microsoft, Amazon, DocuSign und Google. So wurden zum Beispiel allein 2022 mehr als 30 Millionen Phishing-Nachrichten versendet, die scheinbar von Microsoft kamen oder auf Microsoft-Produkte Bezug nahmen*.

Was für Folgen das für Ihr Unternehmen haben kann

Selbst wenige Informationen, die Sie an die Hacker übermitteln, können ausreichen, um an die Daten zu gelangen, die sie benötigen, um auf Ihre Kunden-Accounts zuzugreifen, Passwörter zu stehlen und Sie um Ihr hart verdientes Geld zu bringen.

*Forbes, März 2023

Schulen Sie Ihre Mitarbeiter regelmäßig in Sachen Cybersicherheit und zeigen Sie ihnen dabei vor allem, wie man verdächtige Links erkennt. Denn schon ein einziger Klick kann katastrophale Folgen haben.

Warum die Leute darauf reinfallen

Dieser Trick beruht auf dem Vertrauen, das die meisten von uns den großen Marken entgegenbringen, da wir deren Produkte oft täglich verwenden. Dieses Vertrauen, verbunden mit dem Gefühl der Dringlichkeit, ist es, was die Leute dazu bringt, den Anweisungen von Betrügern Folge zu leisten.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Überprüfen Sie jedes einzelne Mal die E-Mail-Adresse: Hat sie wirklich das richtige Format für das Unternehmen, von dem sie zu kommen scheint?
- Sieht die E-Mail wirklich wie eine echte Mitteilung von der betreffenden Marke aus?
- Wirkt die eingegangene Microsoft-Teams-Nachricht irgendwie verdächtig?
- Enthält die Nachricht Rechtschreib- oder Grammatikfehler?
- Ist wirklich dringend eine Handlung erforderlich? Denn Dringlichkeit sollte Sie immer stutzig machen.

Nur weil LinkedIn eine bekannte Social-Media-Plattform zum beruflichen Austausch ist, ist sie noch lange nicht sicher.

Die Betrugsmasche

Auf LinkedIn tummeln sich leider viele Internetbetrüger. Sie unterbreiten Nutzern falsche Stellenangebote, verwickeln sie in Gespräche über angebliche Bekannte oder fangen sogar zum Schein eine Liebesbeziehung mit ihnen an. Dadurch wollen sie Nutzer dazu verleiten, sensible Daten preiszugeben. Und wenn sie sich das Vertrauen der Zielperson erst einmal erschlichen haben, können sie vielleicht Informationen von ihr bekommen, die sie ihnen sonst nie gegeben hätte.

Warum die Leute darauf reinfallen

Diese Masche beruht auf dem Vertrauen, das wir in professionelle Kommunikationsplattformen wie LinkedIn setzen – und unserer Sehnsucht nach einem Wunder. So unterbreiten die Betrüger den Nutzern zum Beispiel ansprechende Stellenangebote zu verlockenden Bedingungen wie etwa 100 % Homeoffice.

Laut einer jüngsten Studie von Check Point Research* ist LinkedIn sogar die Marke, die von Nachahmern am häufigsten für Phishing-Angriffe missbraucht wird.

* Infosecurity Magazine, April 2022

Was für Folgen das für Ihr Unternehmen haben kann

Wenn es den Betrügern gelingt, persönliche Daten von Ihnen zu bekommen oder Ihnen Schadsoftware (als wichtiges Dokument getarnt) zu schicken, erhalten sie Zugang zu weiteren Daten, wertvollen Dateien oder sogar Geschäftskonten.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Machen Sie allen Mitarbeitern klar, welche Gefahren da draußen auf sie lauern, und schärfen Sie ihnen ein, bei Kontaktaufnahmen Unbekannter (oder scheinbar Bekannter) in den sozialen Netzwerken stets wachsam zu bleiben.
- Hütten Sie sich vor unverlangt zugesandten Mitteilungen.
- Überprüfen Sie die Authentizität aller Dateien, die man Sie auffordert herunterzuladen.

Schärfen Sie Ihren Mitarbeitern ein, sich vor QR-Codes zu hüten, die zur multifaktoriellen Authentifizierung verwendet werden.

Die Betrugsmasche

QR-Codes sind aus unserem Alltag nicht mehr wegzudenken. Deshalb zögern viele Mitarbeiter auch gar nicht lange, wenn sie in einer E-Mail aufgefordert werden, einen QR-Code zu scannen. Doch nicht alle QR-Codes können bedenkenlos gescannt werden.

Fake-Codes erscheinen, auch wenn sie praktisch überall auftauchen können, meist in E-Mails zur multifaktoriellen Authentifizierung oder zum Dokumentenabruf – und manchmal sogar im öffentlichen Raum.

Bei einem erfolgreichen Scam in jüngster Vergangenheit verlor eine ältere Dame sage und schreibe 15.000 EUR, nachdem sie einen Fake-QR-Code gescannt hatte, um ihren Parkplatz zu bezahlen.

Durch diesen Code wurde sie zu einer Fake-Website geleitet, auf der sie brav ihre Zahlungsinformationen eingab. So kamen die Betrüger an ihre Zahlungs- und Kartendaten und konnten sie ausrauben*.

Was für Folgen das für Ihr Unternehmen haben kann

Durch gefakte QR-Codes könnten Betrüger Ihre Mitarbeiter nicht nur zu ihren Websites, Zahlungsportalen und Netzwerken weiterleiten, sondern auch schädlichen Code auf ihre Geräte übertragen, um sensible Daten abzurufen und sie und Ihr Unternehmen um erhebliche Summen zu „erleichtern“.

*Independent, November 2023

Warum die Leute darauf reinfallen

Für viele Unternehmen ist die multifaktorielle Authentifizierung zur täglichen Routine geworden – vor allem im Umgang mit Marken wie Microsoft. Viele Mitarbeiter haben sich so sehr daran gewöhnt, ihre persönlichen Daten irgendwo einzugeben, dass sie das manchmal selbst unter verdächtigen Umständen ohne zu zögern tun.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Überlegen Sie sich gut, welchen QR-Code Sie scannen. Handeln Sie niemals unüberlegt.
- Schauen Sie sich den Link, auf den der QR-Code verweist, vor dem Scannen genau an.
- Vergewissern Sie sich, dass die URL authentisch wirkt und nicht falsch geschrieben ist.
- Scannen Sie keine QR-Codes, die Sie unverlangt von Fremden oder anderen Unternehmen zugeschickt bekommen.
- Wenden Sie sich im Zweifel vorher auf einem anderen Weg an das betreffende Unternehmen.

Mitarbeitern Zugang zu Unternehmens-Accounts zu gewähren, ist zwar praktisch, aber auch riskant. Die darauf basierenden Betrugsfälle haben Unternehmen in den letzten Jahren Millionen von Euro gekostet.

Die Betrugsmasche

Bei dieser Art von Betrug geben Kriminelle vor, Ihre kontoführende Bank zu sein, um an das Geld Ihres Unternehmens zu kommen. Diese Betrugsmasche wird in der Geschäftswelt genauso oft eingesetzt wie im privaten Umfeld, und etwa die Hälfte der Erwachsenen erhält jeden Monat mindestens eine solche Nachricht zu Phishing-Zwecken.

Oft nehmen die Betrüger telefonisch, per Textnachricht oder per E-Mail Kontakt mit Ihrem Unternehmen auf, um Ihnen zum Beispiel zu sagen, dass eine verdächtige Transaktion überprüft werden muss. Dazu sollen Sie auf einen Link klicken, der Sie geradewegs zu einer gefakten Login-Seite führt. Sobald Sie dort Ihre Anmeldedaten eingeben haben, können die Betrüger damit auf Ihr Konto zugreifen. Einige Kriminelle verwenden sogar gefakte Banking-Apps.

Ein bekanntes Opfer dieser Betrugsmasche ist der renommierte britische Haarbürstenhersteller Kent Brushes. Er verlor dadurch innerhalb von nur 20 Minuten ca. 1,8 Millionen EUR. Einer seiner Mitarbeiter wurde von Cyberkriminellen dazu verleitet, ihnen Zugang zum

Was für Folgen das für Ihr Unternehmen haben kann

Sobald sich Internetbetrüger Zugang zu einem Account verschafft haben, können sie weitere Accounts (wie etwa E-Mail-, Bank- oder andere Finanzkonten) hacken.

*BBC.co.uk, Oktober 2023

Warum die Leute darauf reinfallen

Unternehmen vertrauen ihrer Bank ebenso sehr wie Privatleute. Da sie aber auch ständig Angst davor haben, einem Betrug zum Opfer zu fallen, fallen sie leicht auf die Mär von der „verdächtigen Transaktion“ herein.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Denken Sie immer daran, dass Ihre Bank nie von Ihnen verlangen würde, Passwörter preiszugeben oder Geld auf Ihnen unbekannte Konten zu überweisen.
- Verschicken Sie Bankdaten nie per Textnachricht.
- Klicken Sie nie auf unverlangt zugesendete oder verdächtig aussehende Links.
- Überprüfen Sie Bankanmeldeseiten auf Rechtschreib- und Grammatikfehler.

Niemand ist vor Pretexting gefeit. Selbst Ihren Firmenchef kann es treffen. Und je stärker die Zielperson beruflich eingespannt ist, desto größer ist die Wahrscheinlichkeit, dass sie auf die Lügengeschichte hereinfällt, weil sie gerade andere Dinge im Kopf hat.

Die Betrugsmasche

Vielleicht haben Sie schon einmal von einer Betrugsmasche gehört, die sich „Pretexting“ nennt. Dabei nimmt ein Cyberkrimineller unter Vorspiegelung einer anderen Identität (meist der eines Vorgesetzten) Kontakt mit einem Mitarbeiter eines Unternehmens auf und erzählt ihm eine scheinbar glaubwürdige Geschichte, um ihn aufs Glatteis zu führen.

Manchmal verwendet er dazu sogar eine gefakte Sprachaufzeichnung.

Dann verlangt er von diesem Mitarbeiter, ihm sensible Daten zu übermitteln (oder Geld zu überweisen), und droht ihm vielleicht sogar mit Entlassung, wenn er dies nicht tut.

Was für Folgen das für Ihr Unternehmen haben kann

Solche Betrüger recherchieren im Vorfeld genau und verwenden dann richtige Informationen, die sie im Internet oder woanders gefunden haben. Diese richtigen Informationen, die Vertrauen schaffen, ergänzen sie dann durch falsche Telefonnummern und E-Mail-Adressen. Auf diese Weise können sie sich zum Teil erhebliche Summen ergaunern.

Warum die Leute darauf reinfallen

Diese Betrugsmasche beruht auf der Angst vieler Mitarbeiter vor ihren Vorgesetzten und davor, ihren Job zu verlieren. Außerdem schustern sich die Betrüger mithilfe richtiger Informationen eine plausible Geschichte zusammen.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Halten Sie immer kurz inne, um nachzudenken, bevor Sie handeln.
- Verschicken Sie Bankdaten nie per Textnachricht.
- Überlegen Sie sich, ob die Geschichte, die Sie da aufgetischt bekommen, wirklich Sinn macht.
- Kontaktieren Sie die Person, von der die Nachricht zu kommen scheint, auf einem anderen Weg, um herauszufinden, ob die Geschichte stimmt.

Alle Teams, die regelmäßig Geld ausgeben (sei es auch nur für kleine Posten wie Büro-materialien), sollten besonders fit darin sein, Fake-E-Mails und andere Nachrichten von Betrügern zu erkennen. Deshalb sollten Sie sie regelmäßig schulen.

Die Betrugsmasche

Bei dieser Art des Betrugs, die man auch „Business Email Compromise“ oder „BEC“ nennt, geben sich Betrüger als potentielle Kunden aus, bevor sie authentisch wirkende E-Mails an sorgfältig ausgewählte Mitarbeiter schicken. In diesen E-Mails verlangen sie von ihnen, ungewöhnliche Zahlungen vorzunehmen, auf Links (zu betrügerischen Websites) zu klicken oder ihnen bestimmte Produkte zu verkaufen, die sie dann mit gestohlenen Kreditkarten bezahlen.

Im Gegensatz zu den üblichen Phishing-E-Mails, die täglich an Millionen von Leuten geschickt werden, sind BEC-Angriffe genau auf bestimmte Personen zugeschnitten, was es zusätzlich erschwert, sie zu entdecken.

Was für Folgen das für Ihr Unternehmen haben kann

Alle Unternehmen, ob klein oder groß, kann es treffen. 29 % der Unternehmen, die an einer Studie von Security InfoWatch teilgenommen haben, gaben an, schon einmal einen Kunden durch einen BEC-Betrug verloren zu haben*.

2023 fiel MGM Resorts International einem BEC-Betrug zum Opfer, der dazu führte, dass es sein ganzes Computersystem abschalten musste – und dadurch 100 Millionen EUR verlor**.

Mithilfe von Informationen, die er in einem Beitrag auf LinkedIn gefunden hatte, gab sich ein Cyberkrimineller bei seinem Anruf in der IT-Abteilung als MGM-Mitarbeiter aus. Er bat die IT, sein Passwort zurückzusetzen, was sie auch tat. Daraufhin konnte er sich Zugang zum Account dieses Mitarbeiters verschaffen und nach und nach MGMs ganzes System lahmlegen.

Dann hörte alles – von elektronischen Hotelzimmerschlüsseln bis hin zu Spielmaschinen – auf zu funktionieren, und die Webseiten vieler Einrichtungen gingen offline. Gäste mussten stundenlang an der Rezeption anstehen, um einzuchecken und herkömmliche Zimmerschlüssel zu bekommen, oder bekamen handschriftliche Quittungen für Spielcasino-Gewinne ausgehändigt, da das Unternehmen in den manuellen Modus umschalten musste, um seinen Betrieb soweit wie möglich aufrechtzuerhalten.

Warum die Leute darauf reinfallen

Betrüger haben es vor allem auf die Mitarbeiter eines Unternehmens abgesehen, die dafür zuständig sind, Geld auszugeben. Sie machen sich die Angst vieler Unternehmen vor Kostensteigerungen und Ertragseinbußen zunutze und nehmen vor allem Firmen ins Visier, die dringend neue Einnahmen brauchen.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Folgen Sie bei allen Finanztransaktionen Ihren vorgegebenen Richtlinien und Verfahren.
- Seien Sie besonders wachsam bei E-Mails von Unternehmen, mit denen Sie keine Geschäfte tätigen.
- Haben Sie stets ein Auge darauf, welche Informationen über Ihr Unternehmen öffentlich abrufbar sind.
- Überprüfen Sie die Identität der Menschen, die Kontakt mit Ihnen aufnehmen.
- Verwenden Sie für all Ihre Accounts unterschiedliche Passwörter.
- Stellen Sie jede angebliche Dringlichkeit infrage.

*Security InfoWatch, März 2022

**Reuters.com, Oktober 2023

Drucker von Brother sind immer dreifach gesichert und geschützt: auf Netzwerk-, Geräte- und Dokumentenebene.

Die Betrugsmasche

An mehr als einem Zehntel aller Sicherheitsverletzungen in Unternehmen ist ein Drucker beteiligt*. Was wie ein Szenario aus einem billigen Horrorfilm klingt, kann wirklich nervenaufreibend sein. Wenn Hacker erst einmal Ihre Druckerlandschaft übernommen haben, können sie Nachrichten wie „Sie wurden gehackt“ ausdrucken, um Ihnen zu zeigen, wie leicht man in Ihr Netzwerk gelangt.

Was für Folgen das für Ihr Unternehmen haben kann

Leider tun Cyberkriminelle das aber nicht immer nur, um ihre Muskeln spielen zu lassen, sondern manchmal auch, um sich Zugang zu Ihrem Firmennetzwerk zu verschaffen und so weitaus folgenschwerere Angriffe zu verüben. Schließlich können sie sich über Ihre Drucker Zugang zu wesentlich wichtigeren Ressourcen wie Datei- und E-Mail-Servern verschaffen.

*Quocirca, Oktober 2023

Warum die Leute darauf reinfallen

Viele Unternehmen halten Drucker für wenig risikobehaftet – aber da irren sie sich gewaltig. Denn die sensiblen Daten, die Drucker übertragen, könnten Hacker als offenes Hintertürchen in Ihr ganzes Unternehmen betrachten.

Das heißt: Wenn Ihre Drucker sicher konfiguriert sind, sollte niemand in der Lage sein, sich Zugang zu Ihren Geräten zu verschaffen. Achten Sie deshalb stets darauf, dass Ihre Firmware aktuell ist und all Ihre Drucker geschützt sind.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Verhindern Sie den Zugriff unbefugter Nutzer auf Ihre Drucker.
- Verlangen Sie von allen, die Druckerschnittstellen benutzen wollen, sich vorher zu authentifizieren.
- Verwenden Sie starke Passwörter.
- Verlangen Sie die Verschlüsselung von Daten bei ihrer Übertragung, um zu verhindern, dass sie abgefangen und dass Drucker manipuliert werden.
- Halten Sie Ihre Firmware stets auf dem neusten Stand.

Schützen Sie Ihre Daten durch die altbekannten, bewährten Maßnahmen – von der Installation eines starken Virenschutzprogramms bis hin zum umfassenden Schutz Ihres drahtlosen Firmennetzwerks.

Die Betrugsmasche

Das ist vielleicht die Masche in unserer Liste, die die gravierendsten Folgen hat. Dabei nehmen Cyberkriminelle Großkonzerne (oft aus dem Gesundheitswesen, Finanz- oder Energiesektor) ins Visier, um große Mengen an sensiblen Daten zu stehlen, die sie dann „in Geiselhaft nehmen“.

Um Zugang zu diesen Daten zu erhalten, verwenden sie oft Methoden wie Phishing, Identitätsdiebstahl und Sicherheitslücken im System.

Anfang 2023 wurde Großbritanniens Postdienst Royal Mail Opfer eines verheerenden Ransomware-Angriffs durch eine Gruppe von Kriminellen, die drohten, die gestohlenen Daten im Internet zu veröffentlichen. Dadurch war Royal Mail mehr als 2 Wochen lang nicht mehr imstande, Pakete und Briefe ins Ausland zu schicken*.

Was für Folgen das für Ihr Unternehmen haben kann

In den meisten Ländern sind Unternehmen gesetzlich dazu verpflichtet, die personenbezogenen Daten in ihrem Besitz zu schützen – und da Datenschutzverletzungen meist durch erhebliche Geldstrafen geahndet werden, kann es sie teuer zu stehen kommen, in dieser Hinsicht zu versagen. Im Moment verursacht eine Datenschutzverletzung im Durchschnitt Kosten von ca. 5,1 Millionen EUR**.

Eine der folgenschwersten Datenschutzverletzungen der jüngsten Vergangenheit ereignete sich in Großbritannien, als Kriminelle die Wahlkommission angriffen und sich Zugang zu den personenbezogenen Daten von rund 40 Millionen Wahlberechtigten verschafften. Auch wenn sie diese Daten (zum Glück) scheinbar nicht zu anderen Zwecken benutzt haben, hat die bloße Tatsache, dass sie sich Zugang zu ihnen verschaffen konnten, gezeigt, dass das Sicherheitssystem zu schwach war***.

*The Guardian, Januar 2023 **IBM, Januar 2023

Warum die Leute darauf reinfallen

Kriminelle nutzen die Sicherheitslücken von Unternehmen – wie etwa schwache, manipulationsanfällige E-Mail-Systeme, falsch konfigurierte Cloud-Dienste, ungepatchte Schwachstellen und zu wenig Sicherheitsschulungen.

Täglich lesen wir neue Berichte über Datenschutzverletzungen in einigen der größten Unternehmen der Welt. Niemand ist davor gefeit. Und oft werden diese Vorfälle streng geahndet – von hohen Geldbußen bis hin zu Haftstrafen.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Bauen Sie Sicherheitsmaßnahmen in jede Phase der Softwareentwicklung und -bereitstellung ein und testen Sie regelmäßig die Wirksamkeit dieser Maßnahmen.
- Verwenden Sie moderne Technologien zum Datenschutz und zur Compliance, die die Daten auf ihrem Weg durch Datenbanken, Anwendungen und Dienste effektiv schützen.
- Stellen Sie ein Team umfassend geschulter Sicherheitsprofis zusammen, das in kürzester Zeit auf Sicherheitsvorfälle reagieren und ihre negativen Folgen verringern kann.
- Führen Sie solide Praktiken und umfassende Schulungen zum Thema Datenschutz und -sicherheit ein.

Auch wenn es noch so verlockend sein mag, mal einen Blick in die gescannten Dokumente anderer Mitarbeiter zu werfen, sollten Sie das auf keinen Fall tun.

(Und außerdem geht Sie das nichts an!)

Die Betrugsmasche

Stellen Sie sich vor, Sie erhalten überraschend eine E-Mail von Ihrem Bürodrucker, die Sie darüber informiert, dass ein Kollege von Ihnen gerade ein neues gescanntes Dokument erhalten hat. Alle Angaben scheinen richtig zu sein. Sie enthält sogar eine Mitteilung, dass das Dokument ordnungsgemäß gescannt wurde inklusive einem Urheberrechtsvermerk. Außerdem gibt es zwei Links mit der Option, sich das Dokument entweder anzeigen zu lassen oder herunterzuladen.

Doch das ist in Wirklichkeit eine Phishing-E-Mail.

Warum die Leute darauf reinfallen

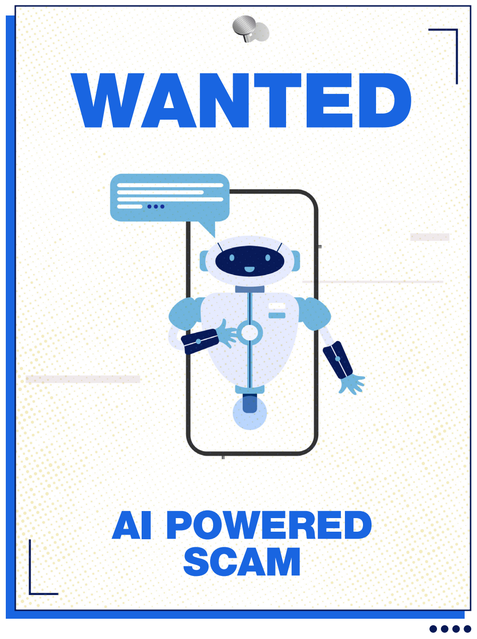
Was diese Phishing-Mails so gefährlich macht, ist, dass sie von einem vertrauenswürdigen Bürogerät kommen, das Sie täglich verwenden. Und da Ihnen dieses Gerät normalerweise keine E-Mails schickt, sind Sie vielleicht so überrascht, dass Sie sich dazu hinreißen lassen, sensible Informationen preiszugeben.

Was für Folgen das für Ihr Unternehmen haben kann

Über die Links werden Sie auf eine Fake-Website von Betrügern geleitet, die versuchen werden, an Ihre E-Mail-Passwörter zu gelangen, um Ihnen danach Spam-Mails zu schicken, Malware aufzuspielen oder Finanzdaten zu stehlen.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Hüten Sie sich vor Anhängen und Links in unerwarteten E-Mails.
- Laden Sie nur Dateien herunter, die nachweislich von vertrauenswürdigen Quellen stammen.
- Stellen Sie jede angebliche Dringlichkeit infrage.



Durch KI-Tools wie ChatGPT wird es immer schwerer, Phishing-E-Mails als solche zu erkennen. Das erhöht die Gefahr für Unternehmen.

Die Betrugsmasche

Wir alle wissen, wie man eine Phishing-Mail erkennt: Sie ist voller Rechtschreib- und Grammatikfehler, stimmts? Tja, die Zeiten sind leider vorbei. Inzwischen verwenden Kriminelle Künstliche Intelligenz und Chatbots, um Sie in perfektem Deutsch „abzufishen“.

Warum die Leute darauf reinfallen

Je authentischer die Phishing-E-Mails erscheinen, desto mehr Menschen werden sich von ihnen hinreißen lassen, personen- und kontobezogene Daten preiszugeben.

Was für Folgen das für Ihr Unternehmen haben kann

Dank solcher Hilfsmittel wirken ihre Schreiben authentischer, Respekt einflößender und vertrauenswürdiger. Und sobald sich die Kriminellen einmal Ihr Vertrauen erschlichen haben, werden sie sich weitere persönliche Informationen beschaffen, um sich die Identität bekannter Personen anzueignen oder auf deren Account zuzugreifen. In der Zeit vom vierten Quartal 2022, als ChatGPT eingeführt wurde, bis Ende November 2023 ist die Anzahl der betrügerischen Phishing-E-Mails um 1.265 % gestiegen*.

Wie Sie Ihr Unternehmen und Ihre Kollegen schützen können

- Halten Sie all Ihre Mitarbeiter über die drohenden Gefahren auf dem Laufenden.
- Achten Sie genau darauf, welche Informationen Ihre Mitarbeiter mit anderen teilen.
- Geben Sie keine Anmeldedaten und Passwörter preis.
- Kontrollieren Sie Ihre öffentlich einsehbaren Daten, da Angreifer sie gegen Sie verwenden könnten.
- Überprüfen Sie die Identität der Menschen, die Kontakt mit Ihnen aufnehmen.

*CNBC, November 2023

Schützen Sie Ihr Unternehmen dauerhaft vor den 10 am häufigsten verwendeten Betrugsmethoden.

Nun sollten Sie wissen, wie Sie die Verhaltensweisen, Taktiken und Tricks von Cyberkriminellen erkennen und durchschauen können.

Doch weil die Folgen eines einzigen Cyberangriffs so gravierend sein können, dass 60 % der kleinen und mittelgroßen Unternehmen innerhalb von 6 Monaten nach einem solchen Angriff ihr Geschäft aufgeben mussten, sollten Sie diesen Leitfaden immer mal wieder zur Hand nehmen, um Ihr Wissen aufzufrischen. Halten Sie ihn am besten griffbereit und geben Sie ihn an Ihre Kollegen weiter.

Denn mit Brother „At your side“ sind Sie den Internetbetrügern immer eine Nasenlänge voraus und können Ihr Unternehmen so langfristig schützen.

brother
at your side