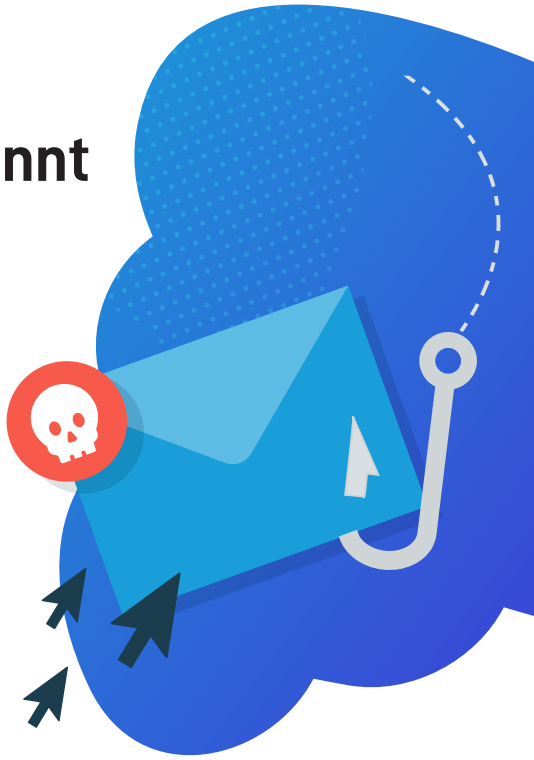
Phishing-Angriffe: Wie man sie erkennt und seine Geschäftsdaten schützt



Die Internetkriminalität nimmt zu, und Hacker nehmen jede Gelegenheit wahr, um ein unwissendes Opfer auszunutzen und Zugang zu persönlichen Informationen zu erhalten, mit der Absicht finanzielle Vorteile zu erzielen. Durch die neue Welt der „Arbeit von überall" ist jeder dem Risiko von Cyberangriffen ausgesetzt.

Eine häufig verwendete Taktik ist Phishing. Phishing-Nachrichten werden mit dem Ziel verfasst, sich die vertraulichen Daten von Personen oder Unternehmen zu verschaffen. Wenn Ihre Mitarbeiter Phishing-Betrug zum Opfer fallen, kann dadurch Ihr Unternehmensnetzwerk beeinträchtigt werden, indem Malware und Viren über Internetverbindungen übertragen werden.

Eine Phishing-E-Mail kann Ausfallzeiten für Ihr gesamtes Unternehmen verursachen und kostet – bedauerlicherweise – kleine Unternehmen durchschnittlich 53.987 €. Je ausgeklügelter die Scams werden, umso schwieriger wird es, sie zu erkennen. Bereiten Sie Ihr Team auf zukünftige Bedrohungen durch Phishing vor, indem Sie lernen, wie man Phishing-Versuche erkennt, bevor sie zu einem Problem werden.

Hier sind fünf verschiedene Arten von Phishing-Angriffen, die Sie vermeiden sollten:

1. Massenkampagnen

Phishing-E-Mails, in denen die Empfänger dazu aufgefordert werden, ihre Anmeldeinformationen oder Kreditkartendaten anzugeben, werden großflächig von betrügerischen Unternehmen versendet. Angriffe, die auf E-Mail-Spoofing basieren, erwecken den Eindruck, von einem vertrauenswürdigen Absender zu stammen; es gibt jedoch verräterische Anzeichen, auf die Sie achten sollten:

- Erscheinen die angegebenen Informationen glaubwürdig? Halten Sie Ausschau nach Dingen wie Rechtschreibfehlern oder einer Absender-E-Mail-Adresse mit der falschen Domain.
- Überprüfen Sie die Nachricht auf Logos, die seltsam oder gefälscht aussehen.
- Ignorieren Sie E-Mails, die nur aus einem Bild und sehr wenig Text bestehen.

2. Spear-Phishing

Ein bestimmtes Unternehmen oder eine bestimmte Person wird direkt zum Opfer gezielter Phishing-E-Mails.

- Achten Sie auf interne Anfragen, die von Personen aus anderen Abteilungen stammen oder anderweitig ungewöhnlich für die jeweilige Rolle erscheinen.
- Seien Sie besonders vorsichtig bei Links zu gespeicherten Dokumenten oder geteilten Laufwerken wie Google Suite, O365 und Dropbox, da diese Sie auf gefälschte, schädliche Websites umleiten können.
- Bei allen gesendeten Dokumenten, die einen Benutzer dazu auffordern, eine Login-ID und ein Passwort einzugeben, könnte es sich um einen Versuch handeln, Anmeldeinformationen zu stehlen.
- Klicken Sie nicht auf einen Link zu einer angeblich bekannten Website. Gehen Sie stattdessen zu Ihrem Browser und wählen Sie von dort aus selbst die Website an. Auf diese Weise können Sie sicher sein, dass Sie zur echten Website gelangen und nicht zu einer Phishing-Version.

3. Whaling

Whaling bezeichnet Spear-Phishing-Angriffe, die sich direkt gegen leitende Angestellte und andere einflussreiche Ziele richten, um Zugriff auf Unternehmensplattformen oder Finanzinformationen zu erhalten.

- Wenn eine leitende Führungskraft noch nie Kontakt zu Ihnen aufgenommen hat, seien Sie skeptisch, ehe Sie die angeforderte Tätigkeit ausführen.
- Stellen Sie sicher, dass jede normal erscheinende Anfrage an eine berufliche und keine private E-Mail-Adresse gesendet wurde.
- Wenn die Anfrage dringend wirkt, könnte es schwerwiegende Konsequenzen haben, sollte sie sich als gefälscht erweisen. Senden Sie eine separate E-Mail/Textnachricht oder rufen Sie den Adressaten an, um die Anforderung zu bestätigen. Gehen Sie lieber auf Nummer sicher.

4. Clone-Phishing

Der Angreifer kopiert eine echte E-Mail-Nachricht von einem vertrauenswürdigen Unternehmen und fügt einen Link ein, der den Empfänger auf eine schädliche/gefälschte Website weiterleitet.

- Seien Sie skeptisch, wenn Sie unerwartet E-Mails von einem Service Provider erhalten, selbst dann, wenn diese Teil der alltäglichen Kommunikation sein könnten.
- Seien Sie vorsichtig, wenn Sie E-Mails erhalten, in denen persönliche Informationen angefordert werden, die Sie bei diesem Service Provider nie zuvor angeben mussten. Wenn Sie sicher sind, dass die Anforderung ihre Richtigkeit hat, ist es am besten, die Website über den Browser aufzurufen und die Daten direkt auf der entsprechenden Seite einzugeben.

5. Pretexting

Beim Pretexting nimmt ein Angreifer zunächst über einen Nicht-E-Mail-Kanal Kontakt auf (z. B. per Voicemail), damit Sie eine scheinbar legitime Nachricht erwarten, nur um dann eine E-Mail zu senden, die schädliche Links enthält.

Was ist zu tun, wenn Sie glauben, eine Phishing-E-Mail erhalten zu haben?

Social Engineering ist „die psychologische Manipulation von Personen, damit diese Tätigkeiten ausführen oder vertrauliche Informationen weitergeben". Angreifer nutzen jeden ihnen zur Verfügung stehenden Trick, um Personen dazu zu bewegen, eine E-Mail zu öffnen, auf Links zu klicken oder eine andere Tätigkeit auszuführen. Beispiele für Social Engineering bei Phishing-E-Mails sind unter anderem:

- Die Aufforderung, auf etwas zu klicken, um etwas zu erhalten.
- Unternehmen, die darauf bestehen, dass ein Passwort aktualisiert werden muss oder Kreditkartendaten veraltet sind.
- Das Erzeugen eines Gefühls von Dringlichkeit.
- Ein Angebot, das Sie nicht erwartet haben.

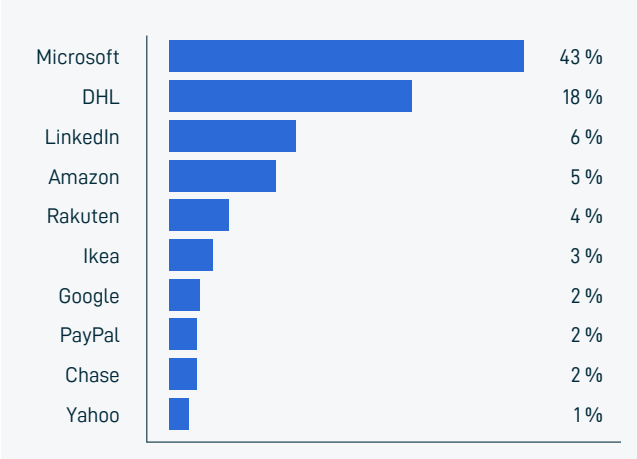
Ist die E-Mail echt oder soll sie nur möglichst echt aussehen?Achten Sie auf Hinweise, von denen sich viele direkt in der E-Mail befinden.

- Überprüfen Sie die tatsächliche E-Mail-Adresse des Absenders.
- Achten Sie auf untypische Grammatik oder Rechtschreibfehler.
- Unerwarteter Absender.

Wenn Sie sich zu der Webseite durchgeklickt haben:

- Passt die URL zur Marke der Webseite?
- Sieht die Seite aus wie die, die Sie erwartet haben?
- Achten Sie auf den Aufbau, die Farben, andere Seiten auf der Site und das Hauptmenü.
- Seien Sie bei den folgenden Marken besonders vorsichtig:

Die führenden Marken, kategorisiert nach ihrem Auftreten von Marken-Phishing-Versuchen im 4. Quartal 2020:



Quelle: *CheckPoint*

Seien Sie vorsichtig! Phishing-Betrüger geben sich als Dateisynchronisierungs- und Freigabeplattformen aus und geben gefälschte Dokumente oder Ordner frei, um Ihren Computer zu infizieren.

Die E-Mail ist immer noch die beliebteste Kommunikationsform im geschäftlichen Kontext, und Phishing-E-Mails sind eine Bedrohung für Unternehmen jeder Art und Größe. Um sich und Ihr Unternehmen zu schützen, ist es wichtig, zu lernen, wie man Phishing-E-Mails erkennt.

Unterbinden Sie Phishing, bevor es überhaupt begonnen hat!

Es ist wichtig, Ihre Mitarbeiter darin zu schulen, wie Phishing-Betrug erkannt werden kann; trotzdem ist es wahrscheinlich, dass früher oder später jemand auf Phishing hereinfällt. Nehmen Sie Kontakt zu uns auf, um zu erfahren, wie die automatisierten Scans von Microsoft-365-E-Mail- und Kollaborations-Tools diese Hacks unterbinden können, bevor sie greifen.

Datto MarketNow | Phone: +1.888.294.6312 | Email: marketnow@datto.com | Datto Inc. | https://www.datto.com

MarketNow