proofpoint.

2025

Kit zum Cybersecurity-Awareness-Monat

Menschenzentrierte bedrohungen jenseits des posteingangs

Ein einmonatiger, kuratierter Leitfaden zur Steigerung des Cybersecurity-Bewusstseins

Jeden Oktober ist der Cybersecurity Awareness Month dem Gespräch mit Ihren Mitarbeitern und Kunden darüber gewidmet, **wie sie sowohl am Arbeitsplatz als auch zu Hause sicher bleiben können.** Wir bei Proofpoint wissen, dass Sie Ihre Planung zeitig beginnen müssen. Starten Sie schnell mit dieser kostenlosen Kampagne und den Inhalten zu menschenzentrierten Bedrohungen.

Diese vierwöchige, kostenlose Sicherheitsbewusstseinskampagne wurde entwickelt, um neue, auf Menschen abzielende Angriffe aufzudecken. **Es soll Ihren Mitarbeitern helfen, zu verstehen, zu erkennen und sichere Entscheidungen zu treffen, wenn sie mit Cyberbedrohungen konfrontiert werden.**

Zum diesjährigen Thema: Menschenzentrierte Bedrohungen jenseits des Posteingangs

Mit der Ausweitung des digitalen Arbeitsplatzes nehmen auch die menschenzentrierten Sicherheitsherausforderungen zu. Während E-Mail weiterhin der primäre Angriffsvektor ist, weiten Cyberkriminelle ihre Angriffe auf andere Kanäle wie Microsoft Teams, Slack, Zoom, LinkedIn und WhatsApp aus.

Sobald Cyberkriminelle ein Konto kompromittiert haben, arbeiten sie daran, ihre Präsenz auszubauen, unentdeckt zu bleiben und weitere Phasen ihres Angriffs einzuleiten.
Dies kann Datenexfiltration, den Einsatz von Ransomware oder finanziellen Diebstahl bedeuten. Während Menschen vielleicht glauben, dass sie auf diesen Plattformen mit einer vertrauenswürdigen Entität interagieren, könnten sie unwissentlich mit einem Bedrohungsakteur in Kontakt treten. Deshalb ist es wichtig, **dass sie neue Angriffsvektoren und Social-Engineering-Taktiken erkennen, um sicherzustellen, dass sie sich selbst und die Organisation schützen können.**

Unser Material dieses Jahr stellt einige Best Practices zur Identifizierung von Bedrohungen vor, die Nutzer über E-Mail und andere digitale Kanäle ins Visier nehmen. Außerdem schult es die Nutzer zu Identitätsanmaßung (Impersonation) und Betrug in der Lieferkette und erläutert die Auswirkungen einer Kontokompromittierung. Es ist die ideale Wahl für den Cybersecurity Awareness Month, kann aber das ganze Jahr über eingesetzt werden.

Informationen zu diesem Kit

Proofpoint hat eine Auswahl kostenloser Lerninhalte aus der Proofpoint ZenGuide Security Awareness Content Library zusammengestellt. Das Kit enthält Messaging für eine einfache Kommunikation sowie einen Ablaufplan für den Start der Kampagne. Wir empfehlen Ihnen, unsere vorgeschlagenen Ressourcen, die Kampagnenkommunikation und den Zeitplan zu prüfen, bevor Sie Ihren Kampagnenansatz finalisieren.

Empfohlene Materialien

Wir haben zentrale Kampagneninhalte ausgewählt, die die heutigen aufkommenden Bedrohungen erklären und aufzeigen, wie Sie sich effektiv schützen können. Videos fördern das Engagement. Deshalb enthält das Kit dieses Jahr fünf sorgfältig ausgewählte Module aus den aktuellen Inhalten, die Proofpoint basierend auf unseren branchenweit führenden Bedrohungsdaten veröffentlicht.

1. **„Bedrohungsübersicht: „Phishing in Messaging-Apps“**

   4-minütiger Überblick darüber, wie Angreifer gezielte Phishing-Angriffe per E-Mail sowie über Kommunikations- und Kollaborationstools wie Microsoft Teams, Slack und Google Chat ausführen

2. **„Zeit, über ... die Lieferkette nachzudenken“**

   Nano-Übersicht, die das Bewusstsein für Angriffe auf die Lieferkette schärft und die Prävention von Lieferantenbetrug thematisiert

3. **„60 Sekunden für mehr Sicherheit: „Was ist Spoofing?“**

   1-minütiger Überblick über E-Mail-Spoofing, Tipps zur Erkennung gefälschter E-Mails und dazu, wie Angreifer diese Methode der Identitätsanmaßung einsetzen

4. **„Anmerkungen eines Experten: Business Email Compromise (BEC)“**

   3-minütiges Video eines Proofpoint Threat Research-Experten darüber, warum Angreifer BEC-Betrug verwenden und wie man sie erkennt

5. **„Very Attacked Persons: Protecting Accounts”**

   2-minütiger Überblick darüber, wie und warum Angreifer bestimmte Personen aufgrund ihres Zugriffs auf sensible Daten oder Netzwerke ins Visier nehmen und wie man die Risiken im Zusammenhang mit der Kompromittierung von Konten erkennt und versteht

Planung
Vor dem Start

Einen Monat vorher

- Sehen Sie sich unsere empfohlenen Ressourcen und Mitteilungen an, um zu entscheiden, was Sie während Ihrer Kampagne verwenden werden und was nicht.
- Identifizieren Sie Ihre Übermittlungsmethoden für Inhalte und Kommunikation (z. B. E-Mail, interne Chat-Kanäle, ein gemeinsames Portal und/oder ein internes Wiki).
- Teilen Sie Ihren Plan mit wichtigen Interessenvertretern und Entscheidungsträgern – und korrigieren Sie den Kurs bei Bedarf.
- Arbeiten Sie daran, eine Top-down- und funktionsübergreifende Zustimmung zu erhalten, um die Stimme Ihrer Kampagne zu verstärken.
- Geben Sie Ihr Startdatum, Enddatum und die dazwischen liegenden wichtigen Meilensteindaten an.

Erstellen Sie ein zentrales Inhaltsrepository

Wir empfehlen die Verwendung eines zentralen Repositorys – beispielsweise eines internen Wikis – für alle benutzerorientierten Lernressourcen in der Kampagne. Dadurch entfällt die Notwendigkeit, alle Ihre Inhalte per E-Mail oder über Chat-Kanäle zu versenden, und die Mitarbeitenden haben einen zentralen Ort, an dem sie die meisten ihrer zugewiesenen Aktivitäten verwalten können.

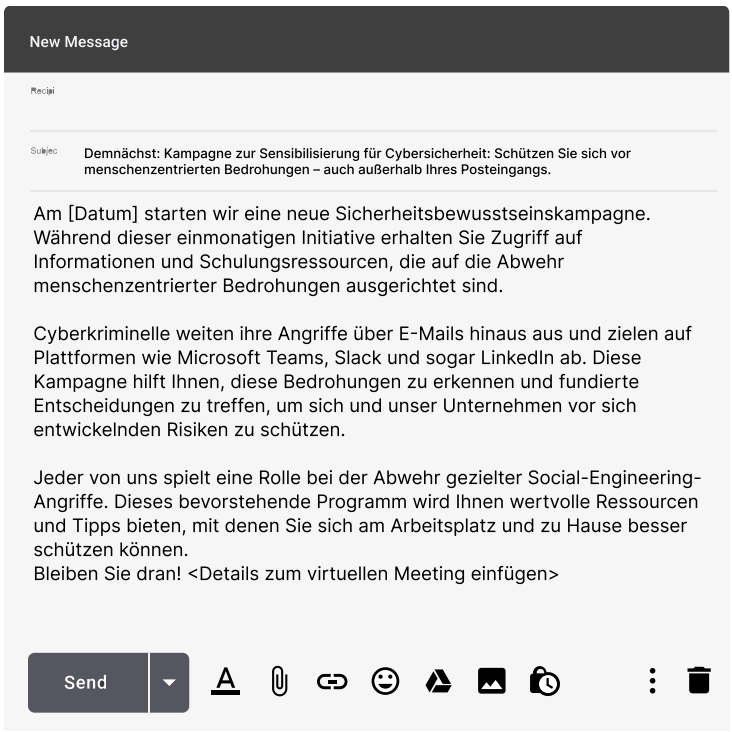
Erstellen Sie einen internen Chat-Kanal

Falls Sie dies noch nicht getan haben, erstellen Sie einen internen Chat-Kanal speziell für Cybersicherheitsbewusstsein und -schulungen. Das bietet Ihnen eine schnelle und einfache Möglichkeit, Erinnerungen an Programmaktivitäten und Meilensteindaten zu versenden.

Eine Woche vorher

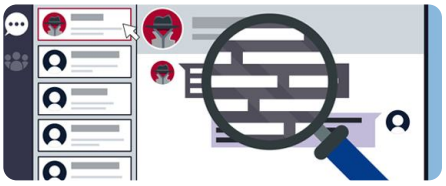
- Kündigen Sie die kommende Kampagne an
- Bereiten Sie in der Woche vor Ihrem offiziellen Start eine Nachricht für die Mitglieder Ihrer Organisation vor. Wir empfehlen, eine unternehmensweite E-Mail mit einer Vorschau auf das kommende Programm zu senden. Wenn möglich, sollte die E-Mail vom CISO oder CEO Ihres Unternehmens versendet werden. was der Kampagne Gewicht sowie Glaubwürdigkeit verleiht und Ihre Bemühungen positiv unterstreicht.

Senden Sie diese empfohlene Mitteilung per E-Mail oder über den internen Chat (bei Bedarf anpassen).



Launch: Woche 1

- Veranstalten Sie eine Kickoff-Sitzung.
- Informieren Sie die Teilnehmer darüber, dass sie wöchentlich E-Mails mit Links zu den Lernmodulen zum Thema Sicherheitsbewusstsein erhalten.
- Fügen Sie in Ihrem Inhaltsrepository das Videomodul **„Bedrohungsübersicht hinzu: Phishing in Messaging-Apps.“**



Assets herunterladen

Senden Sie eine Nachricht per E-Mail oder über interne Chat-Kanäle mit dem folgenden Text (den Sie nach Bedarf ändern können):

New Message

Recipients

Subject Phishing jenseits des Posteingangs

Technische Schutzmaßnahmen können uns nicht immer schützen, daher ist es wichtig, unsere eigene Rolle bei der Sicherheit zu kennen. Sehen Sie sich dieses 4-minütige Video an: „Bedrohungsübersicht: „Phishing in Messaging-Apps“ – erfahren Sie, wie Angreifer Phishing-Angriffe nicht nur per E-Mail, sondern auch über Microsoft Teams, Slack, Google Chat und andere Messaging-Tools durchführen.

Lernen Sie, bösartige Nachrichten zu erkennen, die über alltägliche Kommunikations- und Kollaborationstools übermittelt werden, und denken Sie daran: Nicht alle Kanäle verfügen über herkömmliche Sicherheitskontrollen. Bleiben Sie wachsam und lassen Sie sich nicht ködern!

Greifen Sie so bald wie möglich über den folgenden Link auf das Video zu. Sie sollten es sich ansehen, um den vollen Nutzen aus dem weiteren Material zu ziehen, das wir diesen Monat mit Ihnen teilen!

<[insert link]>

Send

Ermutigen: Woche 2

- Ermutigen Sie die Teilnahme schon früh in Woche 2
- Fügen Sie das Videomodul **„Zeit zum Nachdenken“ hinzu: Die Lieferkette.“**

Assets herunterladen

Senden Sie eine Nachricht per E-Mail oder über interne Chat-Kanäle mit dem folgenden Text (den Sie nach Bedarf ändern können):

New Message

Recipients

Subject Zeit zum Nachdenken: Die Lieferkette

Mittlerweile sollten Sie sich das Awareness-Video angesehen haben, das wir letzte Woche geteilt haben. (Falls Sie das noch nicht getan haben, tun Sie das bitte heute!)

Heute sehen wir uns ein kurzes Video an: „Zeit zum Nachdenken über:“ „Die Lieferkette“ dient als Erinnerung daran, auf Lieferkettenangriffe aufmerksam zu sein. Das Thema ist Lieferantenbetrug und verdeutlicht das Risiko von kompromittierten Lieferantenkonten, die zum Ausnutzen Ihrer vertrauensvollen Geschäftsbeziehungen verwendet werden könnten.

<[Link einfügen]>

Send

Applaus: Woche 3

- Fügen Sie zu Beginn der dritten Woche zwei Videomodule hinzu:
- **„60 Sekunden für mehr Sicherheit: Was ist Spoofing?“** (Woche 3, Teil 1)
- **„Anmerkungen eines Experten: Business Email Compromise.“** (Woche 3, Teil 2)

Assets herunterladen

Senden Sie eine Nachricht per E-Mail oder über interne Chat-Kanäle mit dem folgenden Text (bei Bedarf anpassbar).

New Message

Recipients

Subject 60 Sekunden für mehr Sicherheit: Was ist Spoofing?

Herzlichen Glückwunsch an alle, die das Informationsmaterial zum Thema Cybersicherheit in diesem Monat nutzen.

Wir haben eine neue Ressource zu <[Link einfügen]> hinzugefügt: „60 Sekunden für mehr Sicherheit: Was ist Spoofing?“ Dieses Video bietet eine grundlegende Erklärung zum E-Mail-Spoofing: Dabei fälschen Angreifer die Absenderadresse, sodass eine Nachricht den Anschein erweckt, von einem seriösen Unternehmen, einer Institution oder einer Person zu stammen. Dies ist eine von mehreren Methoden der Identitätsfälschung, die von Angreifern eingesetzt werden, um eine Person dazu zu bringen, Zugangsdaten, Finanzinformationen oder persönliche Daten preiszugeben.

Send

- Teilen Sie später in der Woche ein zweites Video, Woche 3, Teil 2, **„Anmerkungen eines Experten: Business Email Compromise (BEC)“-**Angriffe**.**

Assets herunterladen

Senden Sie eine Nachricht per E-Mail oder über interne Chat-Kanäle mit dem folgenden Text (bei Bedarf anpassbar).

New Message

Recipients

Subject Anmerkungen eines Experten: Business Email Compromise

Herzlichen Glückwunsch zu Ihren Fortschritten in Woche 3 des Materials zur Sensibilisierung für Cybersicherheit in diesem Monat.

Wir haben eine neue Ressource zu <[Link einfügen]> hinzugefügt: „Anmerkungen eines Experten: Business Email Compromise (BEC). In diesem Video erfahren Sie von einem Experten von Proofpoint Threat Research mehr über Business Email Compromise (BEC)-Angriffe, die häufig mit gefälschten E-Mails und Versuchen verbunden sind, Mitarbeiter, Partner oder Kunden dazu zu verleiten, Geld zu überweisen oder vertrauliche Daten preiszugeben.

Send

Abschluss: Woche 4

- Fügen Sie zu Beginn dieser letzten Woche das Videomodul **„Very Attacked Persons hinzu: Protecting Accounts“**
- Senden Sie eine Mitteilung, um die Mitarbeitenden daran zu erinnern, alle Aktivitäten abzuschließen, und laden Sie sie zu einem virtuellen Abschlusstreffen ein.

Assets herunterladen

Senden Sie eine Nachricht per E-Mail oder über interne Chat-Kanäle mit dem folgenden Text (bei Bedarf anpassbar).

New Message

Recipients

Subject Schutz vor Kontokompromittierung

Wir hoffen, dass Sie die in diesem Monat bereitgestellten Ressourcen zum Thema Cybersecurity Awareness genutzt haben. Abschließend haben wir ein finales Video mit dem Titel „Very Attacked Persons: Protecting Accounts“ hinzugefügt: „Protecting Accounts.“ <[Link einfügen]> In einem interessanten, zweiminütigen Video erfahren Sie, wie und warum Angreifer gezielt bestimmte Personen aufgrund ihres Zugriffs auf sensible Daten oder Netzwerke angreifen – und wie Sie die Risiken einer Kontokompromittierung erkennen und verstehen können.

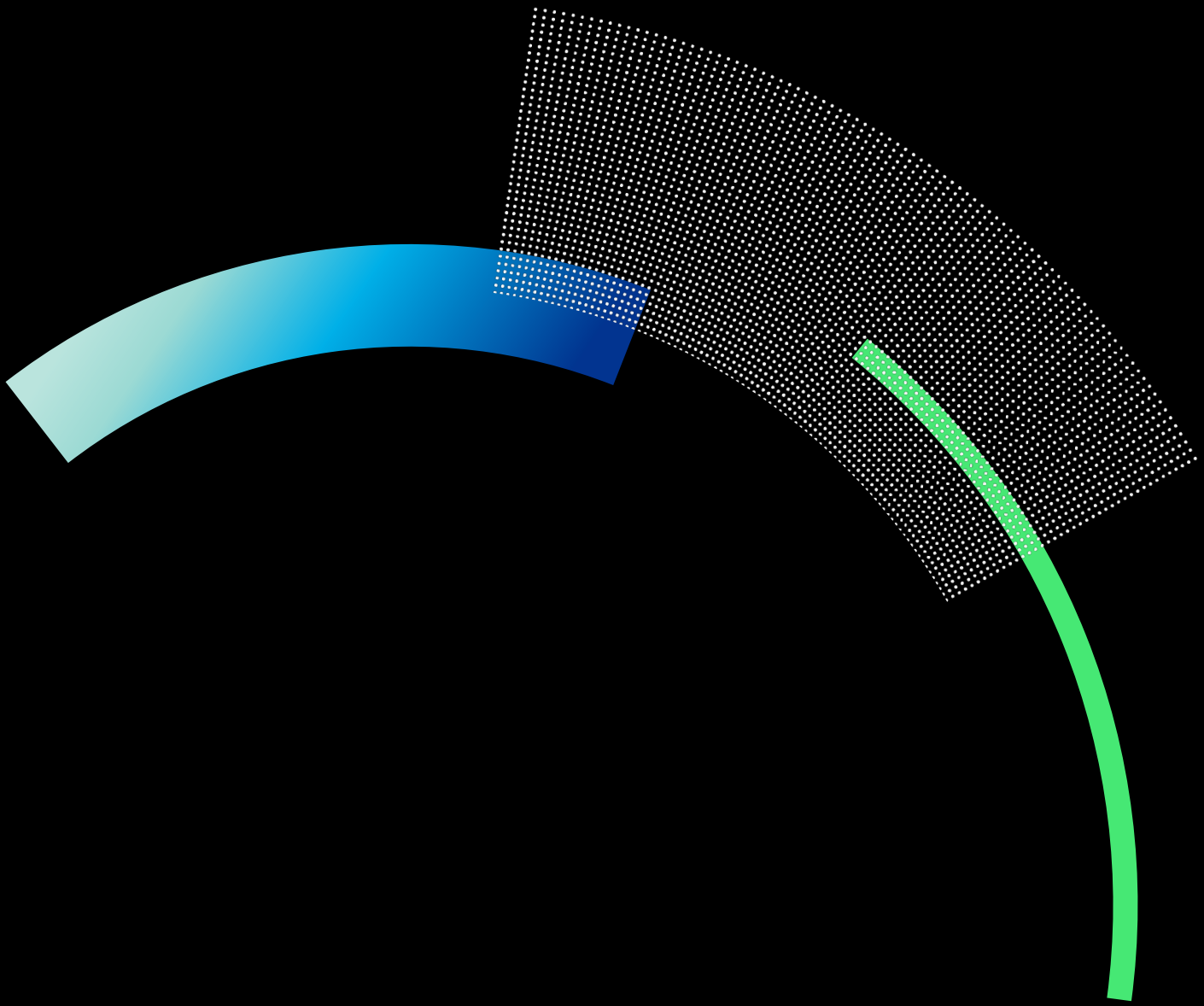
Ich möchte Sie außerdem zu einem virtuellen Abschlusstreffen einladen, bei dem wir Erfolgsgeschichten zu dieser Kampagne besprechen, unsere Teilnehmer würdigen und Sie um Ihr Feedback bitten. <insert meeting details>

Wenn Sie Fragen haben oder Feedback geben möchten, erreichen Sie mich unter <[email]>.

Send

Zeit, die Cybersecurity-Awareness-Kampagne abzuschließen! Öffnen Sie, wenn möglich, die Diskussion zu folgenden wichtigen Punkten:

Was den Teilnehmern an der Kampagne gefallen hat – und was nicht –, welche Erkenntnisse sie gewonnen haben und zu welchen Themen sie gerne mehr erfahren würden Dieses Kit hilft Ihnen, den Monat der Cybersicherheitsaufklärung erfolgreich zu starten und Ihre Mitarbeitenden widerstandsfähiger gegenüber menschenzentrierten, mehrkanaligen und mehrstufigen Angriffen zu machen.



proofpoint.

Proofpoint, Inc. ist ein führendes Unternehmen im Bereich Cybersicherheit und Compliance, das die größten Vermögenswerte und größten Risiken von Organisationen schützt: ihre Mitarbeitenden. Mit einer integrierten Suite cloudbasierter Lösungen unterstützt Proofpoint Unternehmen weltweit dabei, gezielte Bedrohungen abzuwehren, ihre Daten zu schützen und ihre Benutzer widerstandsfähiger gegen Cyberangriffe zu machen. Führende Organisationen aller Größen, darunter 85 % der Fortune 100, verlassen sich auf Proofpoint für menschenzentrierte Sicherheits- und Compliance-Lösungen, die ihre kritischsten Risiken in E-Mails, der Cloud, in sozialen Medien und im Web reduzieren. Weitere Informationen finden Sie unter www.proofpoint.com

Nehmen Sie Kontakt mit Proofpoint auf: LinkedIn

ENTDECKEN SIE DIE PROOFPOINT-PLATTFORM →