proofpoint. | Protect people. Defend data.

Kit zum Cybersecurity-Awareness-Monat 2024: Reporter für Cybersicherheit

Ein speziell zusammengestellter 4-Wochen-Leitfaden zur Bedeutung der Meldung verdächtiger E-Mails im KI-Zeitalter

Jeder Oktober ist Cybersecurity-Awareness-Monat, der Ihre Mitarbeiter und Kunden über sicheres Verhalten informiert – zum eigenen Vorteil sowie zum Schutz Ihres Unternehmens. Wir bei Proofpoint wissen, dass Sie Ihre Planung zeitig beginnen müssen. Beginnen Sie mit dieser kostenlosen Kampagne und Inhalten über die Best Practices zur Identifizierung und Meldung von Phishing-E-Mails.

Über unser Thema

Cyberkriminelle entwickeln ständig neue Angriffsmethoden. Eine Taktik bleibt jedoch immer gleich: Phishing-E-Mails. Da Cyberkriminelle heute zudem generative KI nutzen können, wird die Erkennung von Phishing immer schwerer.

Ihre Mitarbeiter werden verdächtige E-Mails erhalten, in denen sie zum Beispiel aufgefordert werden, auf einen Link zu klicken oder einen Anhang zu öffnen. Es ist wichtig, dass sie die Warnsignale erkennen und wissen, wie sie eine verdächtige E-Mail melden können.

Das Thema „Reporter für Cybersicherheit“ wurde speziell für diese Kampagne erarbeitet. Wir erklären, wie Anwender Phishing erkennen und verdächtige Nachrichten an Ihr Sicherheitsteam melden können. Die Kampagne eignet sich besonders für den Cybersecurity-Awareness-Monat, doch Sie können sie zu einem beliebigen Zeitpunkt starten.

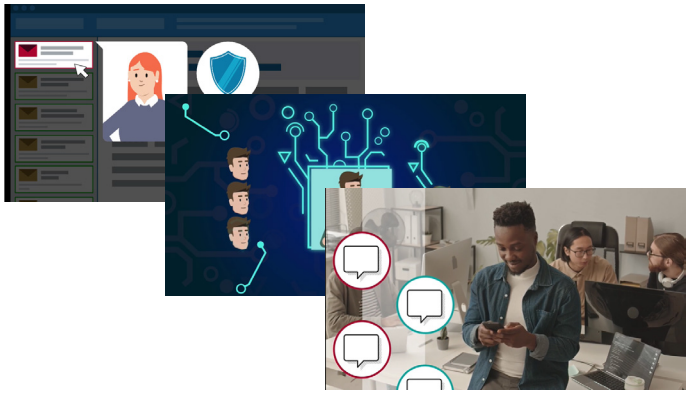
Verwendung dieses Kits

Proofpoint hat eine Auswahl kostenloser Schulungsmaterialien aus unserer Proofpoint Security Awareness-Inhaltsbibliothek zusammengestellt. Mit diesen Materialien steigern Sie die Sensibilisierung für die Abwehr von Phishing-Angriffen, insbesondere von KI-generierten Phishing-Bedrohungen. Das Kit umfasst Kommunikationsvorlagen sowie einen Zeitplan für den Start der Kampagne. Sehen Sie sich unsere Empfehlungen zu den Materialien, zur Kampagnenkommunikation und zum zeitlichen Ablauf genau an, bevor Sie Ihre eigene Kampagne im Detail planen.

Empfohlene Materialien

Videos

Als Kernelemente der Kampagne haben wir Materialien ausgewählt, die verschiedene Phishing-Bedrohungen erläutern und aufzeigen, wie Anwender sich davor schützen können. Videos fördern das Engagement. Deshalb enthält das Kit dieses Jahr drei sorgfältig ausgewählte Videomodule aus den aktuellen Inhalten, die Proofpoint basierend auf unseren branchenweit führende Bedrohungsdaten veröffentlicht.



- **„Reporter für Cybersicherheit: So melden Sie verdächtige E-Mails“**: 2-minütiger, themenbezogener Überblick über grundlegende Informationen zu Phishing-Bedrohungen und wie diese erkannt sowie abgewehrt werden können
- **„Informationen zu Deepfakes“**: 3-minütiger Überblick über KI-generierte Deepfakes und wie diese erkannt sowie abgewehrt werden können
- **„Attack Spotlight: Konversationsbetrug“**: 3-minütiger Überblick über KI-generierten Konversationsbetrug und wie dieser erkannt sowie abgewehrt werden kann

Bilder

Wir haben auch Bilder erstellt, die Sie bei E-Mails, Chat-Kanälen, virtuellen Meetings und anderer Kommunikation verwenden können, um die Information und das Thema aufzugreifen.

- Eine Infografik **„So melden Sie verdächtige E-Mails“**: themenbezogene Infografik mit detaillierten Informationen über schädliche Nachrichten
- Eine animierte GIF **„Reporter für Cybersicherheit“**: themenbezogene Animationen, die Sie auf Ihren digitalen Kanälen teilen können
- Vier Abbildungen **„Sensibilisierung der Reporter für Cybersicherheit“**: themenbezogene Abbildungen zum Untermauern der Schulungsthemen
- Fünf virtuelle Hintergründe **„Reporter für Cybersicherheit“**: themenbezogene Hintergründe zum Dekorieren Ihrer virtuellen Meetings und Videokonferenzen

Alle Materialien sind in 13 Sprachen verfügbar:

- Englisch (USA)
- Arabisch (Ägypten)
- Französisch (Kanada)
- Französisch (Frankreich)
- Deutsch (Deutschland)
- Italienisch (Italien)
- Japanisch (Japan)
- Koreanisch (Südkorea)
- Portugiesisch (Brasilien)
- Spanisch (Spanien)
- Spanisch (Lateinamerika)
- Chinesisch (vereinfacht)
- Chinesisch (traditionell)

Sie haben Zugriff auf alle Design- und Bild-Dateien und können die einzelnen Elemente wie folgt an Ihre eigene Unternehmenskultur anpassen, um das Engagement für das Programm zu steigern:

- Ändern der Asset-Abmessungen für den Druck und die Anzeige in verschiedenen Größen
- Hinzufügen Ihres Unternehmenslogos und Ihrer Markeninhalte
- Bearbeiten des Texts und Ändern der Farben

Ein Monat vor dem Launch

Planen Sie Ihre Kampagne

Bereiten Sie vor dem Start Ihrer Kampagne alles für das große Ereignis vor:

- **Sehen Sie sich unsere empfohlenen Materialien und Kommunikationsvorschläge an** und entscheiden Sie, was Sie nutzen möchten.
- **Passen Sie die Grafikdateien** nach Wunsch an.
- **Wählen Sie die Bereitstellungsmethoden** für Inhalte und Kommunikation (z. B. E-Mail, interne Chat-Kanäle, ein Informationsportal oder ein internes Wiki).
- **Informieren Sie die wichtigsten Projektbeteiligten** sowie Entscheidungsträger und nehmen Sie bei Bedarf Kurskorrekturen vor. Verwenden Sie einen unserer virtuellen Hintergründe zu „Reporter für Cybersicherheit“ für Videokonferenzgespräche.
- **Bemühen Sie sich, Unterstützung durch die Chefetage und andere Abteilungen zu erhalten**, um die Reichweite Ihrer Kampagne zu vergrößern.
- **Legen Sie ein Startdatum**, Enddatum, und das Datum für wichtige Meilensteine dazwischen fest.

Erstellen Sie ein zentrales Content-Repository

Wir empfehlen, ein zentrales Repository (z. B. ein internes Wiki) für alle anwenderorientierten Schulungsressourcen der Kampagne festzulegen. Dadurch müssen Sie nicht alle Inhalte per E-Mail oder über Chat-Kanäle verteilen und können Mitarbeitern einen zentralen Ort bereitstellen, an dem sie die meisten zugewiesenen Aktivitäten verwalten können.

Erstellen Sie einen internen Chat-Kanal

Falls noch nicht geschehen, erstellen Sie einen internen Chat-Kanal explizit für Cybersecurity-Awareness- und Schulungsprogramme. Das bietet Ihnen eine schnelle und einfache Möglichkeit, Erinnerungen über Programmaktivitäten und Meilensteine zu kommunizieren.

Eine Woche vor dem Launch

Kündigen Sie die geplante Kampagne an

Wir empfehlen, eine Woche vor dem offiziellen Launch an alle Personen im Unternehmen eine E-Mail zu senden, in der das geplante Programm vorgestellt wird. Diese E-Mail sollte möglichst vom CISO oder CEO Ihres Unternehmens kommen, was der Kampagne Gewicht sowie Glaubwürdigkeit verleiht und Ihre Bemühungen positiv unterstreicht.

- Teilen Sie die animierte GIF „Reporter für Cybersicherheit“ und diese Vorlagen für die Kommunikation per E-Mail oder über Ihr internes Chat-System (und nehmen Sie nach Bedarf Änderungen vor):

BETREFF:
Demnächst: Reporter für Cybersicherheit

Am <Datum> starten wir eine neue Security-Awareness-Kampagne mit dem Namen „Reporter für Cybersicherheit“. Während dieses 4-wöchigen Programms haben Sie Zugriff auf Informations- und Schulungsmaterialien und erfahren, warum Sie verdächtige Nachrichten, die ein enormes Risiko für Unternehmen und Menschen weltweit darstellen, melden müssen.

Beim Schutz vor Phishing-E-Mails und anderen Cyberangriffen ist jeder gefragt. Im Rahmen dieses Programms erhalten Sie interessante Materialien und wertvolle Tipps dazu, wie Sie sich auf Arbeit und zu Hause besser schützen können.

Bleiben Sie gespannt! *<Fügen Sie Details zum virtuellen Meeting hinzu>*

1. WOCHE

Druckfrisch! Melden Sie verdächtige E-Mails

Starten Sie Ihr Programm

- Veranstalten Sie ein Kickoff-Meeting und verwenden Sie dabei einen virtuellen Hintergrund, um auf das Thema einzustimmen.
- Informieren Sie die Anwesenden darüber, dass sie jede Woche E-Mails mit Links zu den Materialien zum Thema „Reporter für Cybersicherheit“ erhalten werden.
- Fügen Sie das Videomodul „Reporter für Cybersicherheit: So melden Sie verdächtige E-Mails“ und die Abbildung „Schlucken Sie nicht den Köder“ zu Ihrem Content-Repository hinzu.
- Senden Sie eine Kommunikation per E-Mail oder über Ihr internes Chat-System mit dem folgenden Text (den Sie nach Bedarf ändern können):

  BETREFF:
  Druckfrisch! Melden Sie verdächtige E-Mails

  Technische Schutzmaßnahmen bieten keine vollständige Sicherheit. Deshalb ist es wichtig, die Rolle von uns allen bei der Absicherung zu kennen. In diesem 2-minütigen Video zum Melden verdächtiger E-Mails erhalten Sie grundlegende Informationen zu Phishing-E-Mails, wie Sie diese erkennen und wie Sie sich vor ihnen schützen können. Denken Sie immer daran: Schlucken Sie nicht den Köder!

  Sehen Sie sich das Video über den folgenden Link zu einem für Sie günstigen Zeitpunkt an. Es ist notwendig, um die übrigen Materialien dieser Woche bestmöglich nutzen zu können. *<[Link einfügen]>*

- Senden Sie nach einigen Tagen die Abbildung als Erinnerung und zum Beispiel folgenden Text:

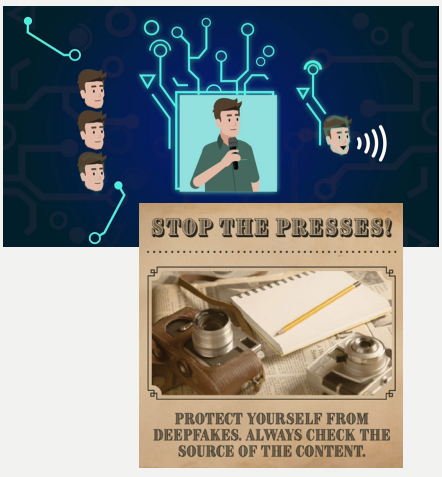
  Schlucken Sie nicht den Köder! Sie sind die letzte Verteidigungslinie, um sich selbst und unser Unternehmen vor Phishing-E-Mails zu schützen. Melden Sie deshalb jede verdächtige E-Mail.

---

2. WOCHE

Hören Sie auf zu klicken! Achten Sie auf Anzeichen für KI (Teil 1)

Fordern Sie zur Teilnahme auf



- Fügen Sie am Anfang der 2. Woche das Videomodul „Informationen zu Deepfakes“ und die Abbildung „Hören Sie auf zu klicken!“ hinzu.
- Senden Sie eine Kommunikation per E-Mail oder über Ihr internes Chat-System mit dem folgenden Text (den Sie nach Bedarf ändern können):

  BETREFF:
  Hören Sie auf zu klicken! Achten Sie auf Anzeichen für KI (Teil 1)

  Mittlerweile sollten Sie sich das Awareness-Video angesehen haben, das wir letzte Woche geteilt haben. (Falls nicht, holen Sie das bitte umgehend nach.)

  Heute sehen wir uns ein weiteres Video an. Diesmal geht es darum, wie generative KI die Erkennung von Phishing erschwert. In nur 3 Minuten erhalten Sie grundlegende Informationen zu Deepfakes und zu einer neuen Methode, mit der Angreifer Sie hereinlegen wollen. *<[Link einfügen]>*

- Senden Sie nach einigen Tagen die Abbildung als Erinnerung und zum Beispiel folgenden Text:

  Hören Sie auf zu klicken! Schützen Sie sich vor Deepfakes. Diese KI-generierte Phishing-Methode kann Autoritätspersonen in Videos, Abbildungen, oder kurzen Sprachaufnahmen imitieren und absichtlich Falschinformationen verbreiten.

3. WOCHE

Extrablatt! Hier erfahren Sie alles

Loben Sie die aktive Teilnahme

- Fügen Sie am Anfang der 3. Woche die Infografik „So melden Sie verdächtige E-Mails“ und die Abbildung „Extrablatt! Quishing-Alarm“ hinzu.
- Senden Sie eine Kommunikation per E-Mail oder über Ihr internes Chat-System mit dem folgenden Text (den Sie nach Bedarf ändern können):

  BETREFF:
  Extrablatt! Hier erfahren Sie alles

  Wir gratulieren allen, die unsere Materialien nutzen und zu Reportern für Cybersicherheit geworden sind.

  Wir haben zu *<[Link einfügen]>* die Infografik „So melden Sie verdächtige E-Mails“ hinzugefügt. Sie geht noch einmal genauer auf die Erkennung und sichere Meldung verdächtiger E-Mails ein, da Angreifer sich immer neue Methoden wie Phishing mit QR-Codes (auch „Quishing“ genannt) ausdenken, mit denen sie uns austricksen können.

- Senden Sie nach einigen Tagen die Abbildung als Erinnerung und zum Beispiel folgenden Text:

  Extrablatt! Quishing-Alarm! Scannen Sie niemals unverlangt zugesendete QR-Codes von unbekannten oder kontextfremden Quellen, egal ob physisch oder elektronisch.

---

4. WOCHE

Wer etwas Verdächtiges sieht, sollte es melden! Achten Sie auf Anzeichen für KI (Teil 2)

Laden Sie zu einem abschließenden Meeting ein

- Fügen Sie am Anfang der letzten Woche das Videomodul „Attack Spotlight: Konversationsbetrug“ und die Abbildung „Melden Sie verdächtige Situationen“ hinzu.
- Erinnern Sie alle Mitarbeiter in einer E-Mail daran, alle Aktivitäten abzuschließen. Vergessen Sie nicht, die Einladung zu einem abschließenden virtuellen Meeting zu versenden.

  BETREFF:
  Wer etwas Verdächtiges sieht, sollte es melden! Achten Sie auf Anzeichen für KI (Teil 2)

  Wir hoffen, dass Sie die Materialien zum Thema „Reporter für Cybersicherheit“, die Sie in den letzten Wochen erhalten haben, nützlich fanden. Zum Abschluss haben wir ein letztes Video „Attack Spotlight: Konversationsbetrug“ hier *<[Link einfügen]>* hinzugefügt. In diesem interessanten 3-minütigen Video dreht sich alles um eine weitere Art von KI-generierten Phishing-Angriffen.

  Denken Sie immer daran, wie es in dieser Abbildung heißt *<[Link einfügen]>*: „Wer etwas Verdächtiges sieht, sollte es melden.“ Melden Sie Sicherheitszwischenfälle unverzüglich, denn mit schnellen Gegenmaßnahmen können weitere Kompromittierungen verhindert werden.

  Ich möchte Sie zu einem abschließenden virtuellen Meeting einladen, bei dem wir Erfahrungen aus dieser Security-Awareness-Kampagne vorstellen, unsere aktivsten und erfolgreichsten Teilnehmer auszeichnen und von Ihnen allen Kommentare und Rückmeldungen einholen. *<Fügen Sie Details zum Meeting hinzu>*

  Falls Sie Fragen oder Anmerkungen haben, senden Sie bitte eine E-Mail an *<[E-Mail-Adresse]>*.

Abschluss Ihrer Kampagne

Durchführung eines abschließenden Meetings

Es nun Zeit ist, die Kampagne zu Ende zu bringen. Nutzen Sie bei diesem Meeting einen der themenbezogenen virtuellen Hintergründe. Wenn möglich, beginnen Sie die Diskussion mit wichtigen Punkten wie den folgenden:

- Was hat den Teilnehmern an der Security-Awareness-Kampagne gefallen (und was nicht)?
- Was haben die Teilnehmer gelernt?
- Zu welchem Thema wünschen sich die Teilnehmer mehr Informationen?

Noch bessere Wirkung?

Werden Sie Proofpoint-Kunde

Dieses Kit zum Cybersecurity-Awareness-Monat gehört zur übergreifenden Kampagne „Reporter für Cybersicherheit“, die exklusiv für Proofpoint-Kunden verfügbar ist. Die komplette Kampagne baut auf den Inhalten in diesem Dokument auf und stellt Ihnen zahlreiche Kommunikationstools und Awareness-Inhalte bereit, die während des dicht gepackten Monats die aktive Teilnahme Ihrer Anwender fördern.

Proofpoint-Kunden haben Zugriff auf umfangreiches nützliches Material wie dieses:

- **Kampagnenleitfaden**, der diesen Dokumentplan um weitere Inhalte und Informationen ergänzt
- **Zusätzliche Module**, die detaillierter auf empfohlene Verhaltensweisen beim Surfen im Web eingehen
- **Postkarten**, mit denen Sie Anwender auf die geplante Kampagne hinweisen und zur Teilnahme auffordern können
- **Aktivitätenübersichten**, in denen Anwender ihre abgeschlossenen Aktivitäten notieren können
- **Abzeichen**, die Sie Anwendern zusenden können, wenn sie die wöchentlichen Aktivitäten durchgeführt haben
- **Incentives** wie ausdruckbare Aufkleber, die als Belohnung für gute Beteiligung verschenkt werden können
- **Inhalte zum Weitergeben** wie Poster, animierte Bildschirmschoner, ein Newsletter mit Tipps und themenbezogene Bilder, die an die während der Kampagne gestellten Aufgaben erinnern sollen

Demo vereinbaren

Weitere Informationen finden Sie unter **proofpoint.de.**

proofpoint.