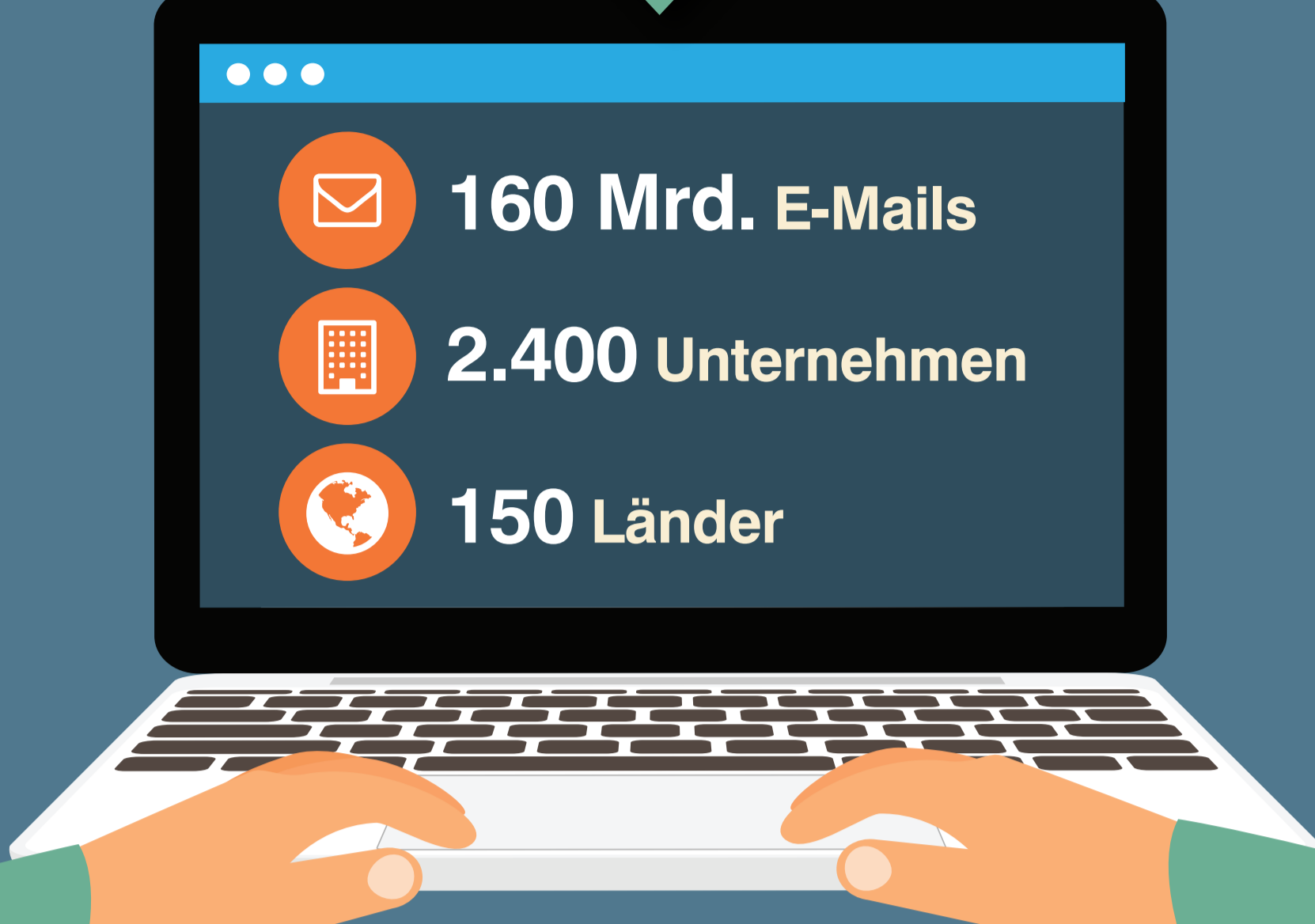


DER ZUSTAND DES E-MAIL-BETRUGS DAS JAHR IM RÜCKBLICK

E-Mail-Betrug ist heutzutage eine der häufigsten Cyberbedrohungen. Um den Umfang des Problems und die angewandten Taktiken besser zu verstehen, hat Proofpoint Folgendes analysiert: mehr als...



Hier sehen Sie einen Schnappschuss unserer Erkenntnisse für 2017.

E-MAIL-BETRUG AUF DEM VORMARSCH

Angreifer bedrohten mehr Organisationen und häufiger als im Vorjahr.



88,8 %

aller Unternehmen wurden von mehr als einer E-Mail-Betrugsattacke angegriffen



18,5

betrügerische E-Mails pro Quartal wurden von den angegriffenen Unternehmen entdeckt

Im 4. Quartal wurden durchschnittlich **13 Mitarbeiter pro Organisation** angegriffen

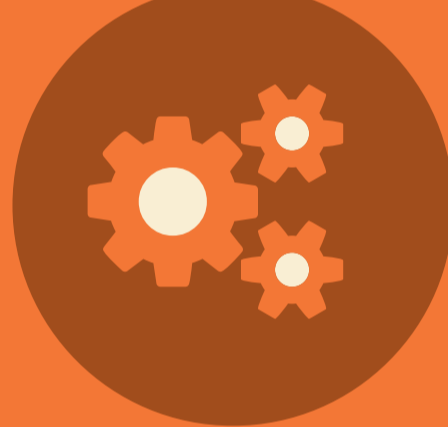
WER SIND DIE ZIELPERSONEN?

E-Mail-Betrug diskriminiert nicht – er greift Unternehmen jeder Größe in allen Branchen an. Hier sind einige der größten Branchen, die von E-Mail-Betrug betroffen waren (nach Angriffen pro Unternehmen 2017):



Finanzdienstleistungen

93



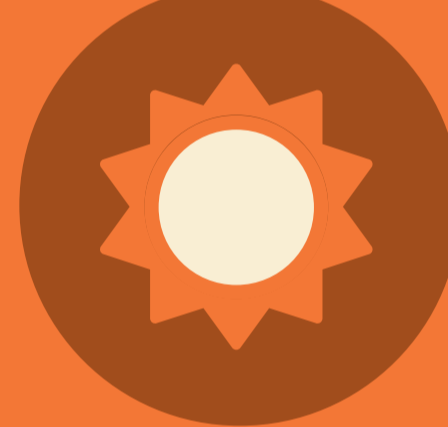
Produktion

159



Gesundheitswesen

79



Versorgungsunternehmen

120

HÄUFIGSTE BETREFFZEILEN FÜR E-MAIL-BETRUG

E-Mail-Betrugsangriffe verwenden alle möglichen Überschriften, um die Empfänger zum Klicken zu verleiten.



Betreffzeilen mit dem Begriff „Rechtsabteilung“ stiegen mit

1.080 %

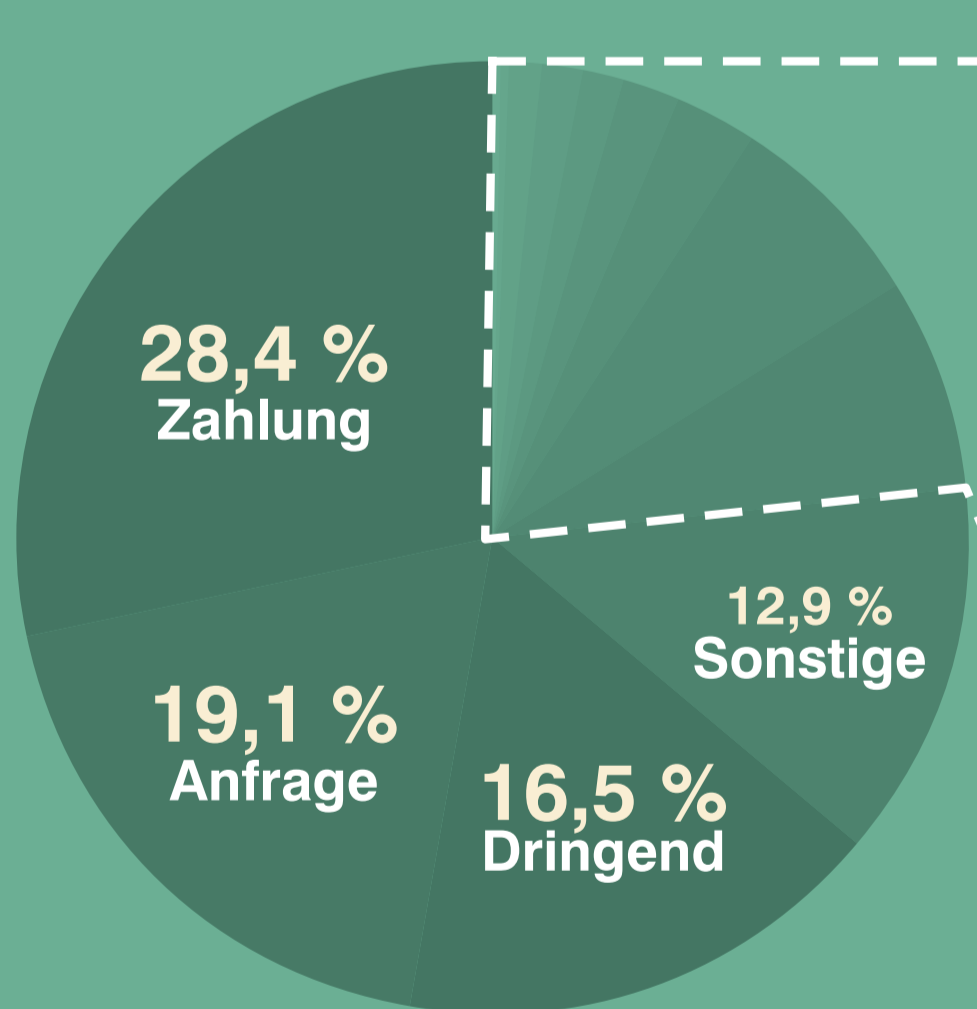
gegenüber dem Vorjahr am meisten an



„Andere“-Betreffs stiegen um

16 %

der gesamten E-Mail-Kopfzeilen



- 7,2 % Begrüßung
- 7,0 % Leere Betreffzeile
- 2,6 % Zur Information
- 2,0 % Wozu gehören Sie?
- 1,4 % Dokument
- 1,4 % Datum
- 1,1 % W2
- 0,2 % Vertraulich
- 0,2 % Rechtsabteilung
- 0,0 % Steuern

HÄUFIGSTE E-MAIL-BETRUGSMETHODEN



Gefälschte E-Mail-Verläufe

Der Prozentsatz an E-Mail-Betrugsbedrohungen mit gefälschten E-Mail-Verläufen stieg im 4. Quartal auf **11 % aller E-Mail-Angriffe** gegenüber **7,31 %** im Vorjahr an.

Domännennachahmung

2017 erlebten **93 % aller Organisationen mindestens eine Domänen-Nachahmungsattacke**, wobei ein Betrüger die vertraute Domäne des Unternehmens verwendet, um andere zu täuschen.



Betrug mit ähnlichen Domänen

Die Angreifer registrieren Domänen, die denen vertrauter Marken verblüffend ähnlich sehen. **Mit 38 % ist der Austausch von Buchstaben die häufigste Methode beim Betrug mit ähnlichen Domänen.**

Lesen Sie hier den vollständigen Bericht proofpoint.com/de/solutions/email-fraud