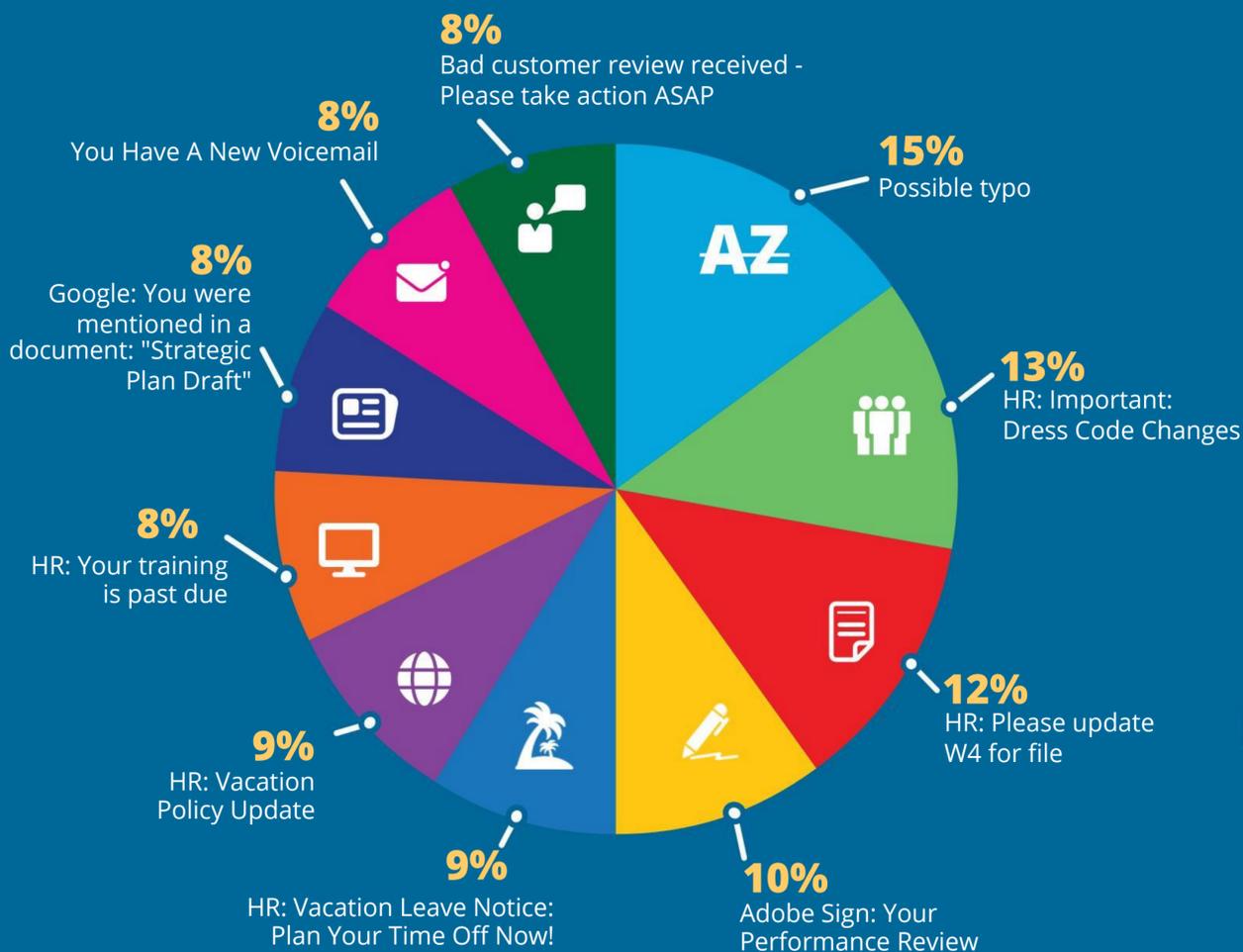


TOP-CLICKED

# PHISHING TESTS

## <一般的に使われるフィッシングメール件名トップ5>



### 注目ポイント

ここ数ヶ月、人事部/IT部門/上司から発信される業務関連のフィッシングメール件名は、様々なテーマを取り扱うようになってきています。このようなテーマは、ユーザーの日常業務に影響を及ぼすことを思わせ、メールの真偽を論理的に考える前に直感的に反応させるため、極めて効果的です。

## <実際のフィッシングメールの件名で最も一般的なもの>

- ✔ LinkedIn: LinkedIn Enhanced Security
- ✔ AWS: AWS Account on Hold: Response Required
- ✔ IT: ChatGPT Demand Survey
- ✔ Voicemail received
- ✔ HR: Director and Employee Evaluation Reports
- ✔ Coinbase: Your Coinbase account is frozen
- ✔ Urgent Request from [[manager\_name]]
- ✔ Microsoft: Time-Sensitive: Renew Your Password N
- ✔ Dropbox: You've received a new document via Drop
- ✔ Zoom: We encountered a problem with your sched



### 注目ポイント

今期のフィッシングメール件名で目立つものは、IT通達やオンライン・サービスのお知らせやLinkedInからのメッセージです。このような業務関連のフィッシングメールを受け取った場合、メールの正当性を論理的にじっくりと考える前に、直感的に反応してしまう傾向があります。そのため、この種の件名は極めて効果的です。

## <攻撃ベクトルのトップ5>



**リンク**  
メール内にフィッシングハイパーリンクを埋め込む



**なりすましドメイン**  
ユーザーのドメインから来たように見せかける



**PDF添付**  
悪意あるPDF添付をメール内に仕込む



**ブランド偽装**  
ロゴや社名を使って、有名企業になりすます



**HTML添付**  
悪意あるHTML添付をメール内に仕込む



### 注目ポイント

これは、KnowBe4のセキュリティ意識向上トレーニングプラットフォームで観測された攻撃ベクトルの上位ランキングです。KnowBe4のフィッシング演習および実際に目撃されたフィッシング攻撃でこの四半期に最も多かった攻撃手口は、これまでと変わりなく、メール本文に埋め込まれたフィッシングリンクです。これらのリンクがクリックされると、多くの場合、ランサムウェアやビジネスメール詐欺(BEC)など、悲惨なサイバー攻撃を発生させます。

## <ホリデーフィッシングメール件名トップ5>

- ✔ Amazon: Save up to 50% off on Halloween
- ✔ Starbucks: Free Pumpkin Spice Latte
- ✔ HR: Halloween costume contest!
- ✔ Walmart: \$10 off Halloween Candy!
- ✔ Hulu: Start Screaming on Hulu Today!



### 注目ポイント

ホリデーシーズンや夏休みなどの特別キャンペーンやクーポンがこれにあたります。また、夏休みスケジュール変更などの人事関連の通達は、休日が増える、勤務時間が短縮される、など、従業員の興味をそそるものです。