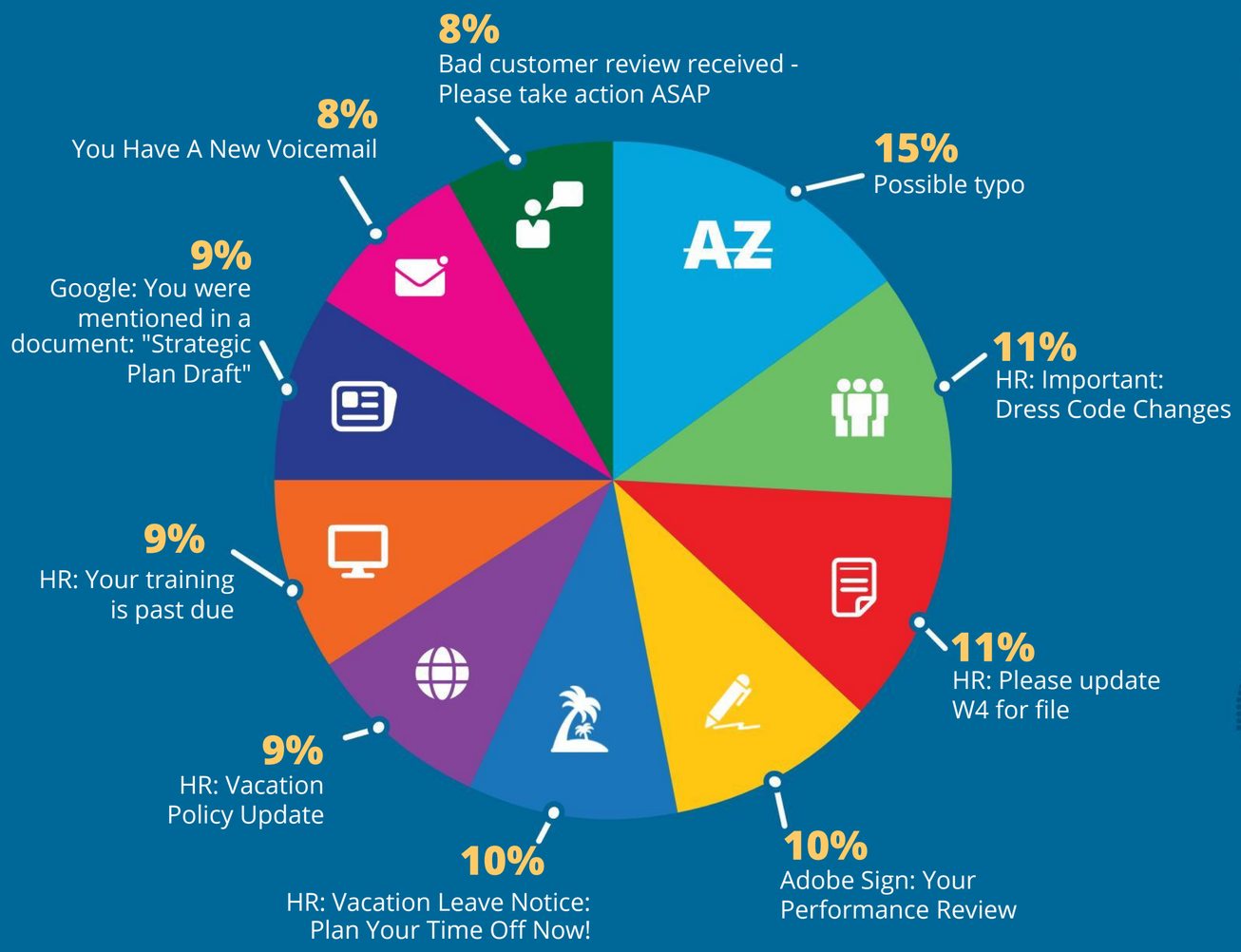
TOP-CLICKED PHISHING TESTS

＜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。業務関連のフィッシングメール件名のほか、もう一つの注目テーマは税金・租税関連です。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。

＜ホリデーフィッシングメール件名トップ5＞

- HR: Change in Holiday Schedule
- HR: Happy 4th of July Message!
- HR: Juneteenth Survey
- HR/July 4th: RSVP for Company BBQ!
- Juneteenth celebration sign-up

注目ポイント
祝祭日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。祭事イベントのお知らせやアンケートの依頼もユーザーのクリックを誘うのに極めて効果的です。

＜実際のフィッシングメールの件名で最も一般的なもの＞

- HR: Staff Rewards Program
- Someone is trying to send you money
- IT: Important Email Upgrades
- ALERT - Mail Redirect Triggered
- Amazon: Action Needed: Purchase Attempt
- Microsoft 365: [[display_name]], MFA Security Review is Required
- A fax has arrived
- Google: [[manager_name]] invited you to join Google Chat Group
- Metamask Wallet Update
- Chase: Confirm Your Card Possession

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。