KnowBe4
Human error. Conquered.

MEEST GEKLIKTE PHISHING-TESTS

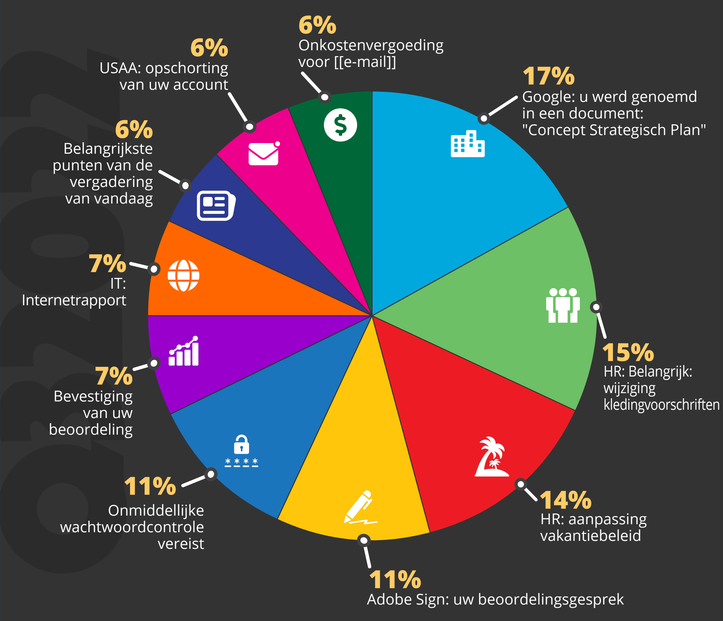
VEEL VOORKOMENDE 'IN-THE-WILD'-AANVALLEN

- Update van apparatuur en software
- E-mailnotificatie: u heeft 5 versleutelde berichten
- Amazon: Amazon - verzending vertraagd
- Google: uw wachtwoord vervalt binnenkort
- Actie vereist: uw betaling is geweigerd
- Wells Fargo: overboeking voltooid
- DocuSign: bekijk en onderteken uw document a.u.b.
- IT: IT-tevredenheidsonderzoek
- Zoom: [[naam_manager]] heeft u een bericht gestuurd via Zoom Message Portal
- Microsoft: beveiligingscode Microsoft-account

BELANGRIJKSTE CONCLUSIE

Deze phishing-tests variëren van berichten die pretenderen van interne afdelingen afkomstig te zijn tot externe verzoeken die een gevoel van urgentie overbrengen om informatie te winnen en gebruikers aan proberen te zetten tot actie.

TOP E-MAIL ONDERWERPEN WERELDWIJD



BELANGRIJKSTE CONCLUSIE

We hebben in de afgelopen maanden veel meer bedrijfsgerelateerde onderwerpen gezien van HR/IT/managers. Andere onderwerpen betreffen het inloggen op nieuwe apparaten en het opnieuw instellen van wachtwoorden. Deze aanvallen zijn effectief omdat ze het dagelijkse werk van gebruikers kunnen beïnvloeden en ervoor zorgen dat iemand meteen reageert voordat hij of zij langer nadenkt over de legitimiteit van de e-mail.

TOP 5 AANVALSVECTOREN

Link
Phishing-hyperlink in de e-mail

Spoofs-domein
Lijkt afkomstig te zijn van het domein van de gebruiker

PDF-bijlage
E-mail bevat een PDF-bijlage

Branded
Phishing-testlink bevat het logo en de naam van de organisatie waar de gebruiker werkzaam is

Landingspagina met referenties
Phishing-link leidt gebruiker naar landingspagina voor gegevensinvoer of aanmelding

BELANGRIJKSTE CONCLUSIE

Dit is een ranglijst van de meest aangetroffen aanvalsvectoren in KnowBe4 Phishing Security Tests. Het is niet verrassend dat phishing-links in de body van e-mails op nummer 1 staat. Deze troffen we 'in-the-wild' en tijdens onze tests het meest aan. Als er op deze links wordt geklikt leiden ze vaak tot rampzalige cyberaanvallen zoals ransomware en zakelijke e-mail compromis.