

Esimerkki täsmäntävästä tiedonhausta tekoälyn avulla

1

Olen kansalaisopiston opettaja. Haluan kertoa opiskelijoille minkälaisia huijauksia Internetissä on tällä hetkellä on. Tee 10 kohdan luettelo yleisimmistä...

◆ Hei, mainio idea! On tärkeää, että opiskelijat ovat tietoisia Internetin vaaroista. Tässä on 10 kohdan luettelo yleisimmistä verkkohuijauksista, joita voit hyödyntää opetuksessasi.

1. Tietojenkalastelu eli phishing

Tämä on ehkä yleisin huijaustyyppe. Huijari lähettää sähköpostiviestin, tekstiviestin tai linkin, joka näyttää tulevan luotettavalta taholta, kuten pankilta, verottajalta tai postipalvelulta. Viestin tavoitteena on saada sinut klikkaamaan linkkiä, joka ohjaa väärennetylle sivustolle. Sivustolla pyydetään antamaan henkilötietoja, kuten pankkitunnuksia tai luottokortin numeroita, jotka huijari varastaa.

2. Valepolliset- ja huijaussoitot

Huijari soittaa uhrille ja esittäytyy poliisiksi tai viranomaiseksi. Hän väittää, että uhrin pankkitiliin on tehty tietomurto tai että tili on vaarassa. Huijari pyytää uhrin siirtämään rahaa "turvaan" tai antamaan pankkitunnuksia, jotta tiliin "ongelma" voidaan korjata. On tärkeää muistaa, että poliisi tai pankki ei koskaan pyydä pankkitunnuksia puhelimesta.

3. Romanssihuujaukset

Huijari luo valehenkilöisyyden ja lähestyy uhrin sosiaalisessa mediassa tai deittisovelluksessa. Hän aloittaa romanttisen suhteen ja luo uhrille vahvan tunnesiteen. Kun luottamus on rakennettu, huijari keksii tarinan, esimerkiksi rahan tarpeesta matkustaakseen tai sairauskulujen vuoksi, ja pyytää uhrilta rahaa.

Kysy Geminiästä

+ Deep Research Video Kuva Canvas

2

gemini.google.com/app/ba6160c59e8bbd3b

Gemini
2.5 Flash

Kerro lisää tekstiviestihuijauksista

◆ Tekstiviestihuijaukset, joita kutsutaan myös nimellä **smishing**, ovat tietojenkalastelua, joka tapahtuu tekstiviestien välityksellä. Nimi smishing tulee sanoista SMS (tekstiviesti) ja phishing (tietojenkalastelu). Se on yksi yleisimmistä ja tehokkaimmista huijaustavälineistä, koska tekstiviestit luetaan usein nopeasti ja niihin suhtaudutaan usein luottavaisemmin kuin sähköposteihin.

Miten smishing-huijaus toimii?

Huijari lähettää tekstiviestin, joka yrittää luoda kiireellisen tai tärkeän vaikutelman. Viesti yrittää saada sinut toimimaan ilman ajattelua. Viesti sisältää yleensä linkin, joka johtaa huijarin luomalle väärennetylle verkkosivulle.

Yleisimpiä aiheita, joita huijarit käyttävät:

- **Postipalvelut tai pakettilähettykset:** Saat viestin, jossa sanotaan, että pakettisi toimitus on keskeytynyt tai että se odottaa maksua. Esimerkiksi "Pakettisi Postissa on pysähtynyt, vahvista osoite ja maksa pieni maksu tästä linkistä."
- **Pankit tai luottokortit:** Viesti varoittaa epäilyttävästä tapahtumasta tiliilläsi tai ilmoittaa, että tili on lukittu turvallisuussyistä. Viestissä pyydetään sinua vahvistamaan tietosi tai kirjautumaan sisään linkin kautta.
- **Veronpalautukset:** Saat viestin, joka lupaa sinulle veronpalautusta. Tämän saadaksesi sinun täytyy antaa pankkitietosi tai luottokortin numeron väärennetyllä verkkosivulla.
- **Arvonnat ja kilpailut:** Ilmoitetaan, että olet voittanut suuren summan rahaa tai kalliin tuotteen ja sinun täytyy antaa tietosi "lunastaksesi" voiton.
- **Netflix, Apple tai muut palvelut:** Viesti ilmoittaa, että tili on jäädytetty tai tilaus on peruutettu ja pyytää sinua päivittämään maksutietosi linkin kautta.

Kyey Geminiä

+ 🔍 Deep Research 📺 Video 🖼️ Kuva 🎨 Canvas ... 🗣️