Prevare na društvenim mrežama

Bruna Matić, 13.11.2024.

Pregled predavanja

- Pojam social engineering
- Što je prevara i koji su njeni najčešći oblici
- Primjeri prevara

Pitanja za ispite

- 1) Što je social engineering?
- 2) Što je scamming?
- 3) Koji su najpopularniji oblici scamminga?
- 4) Kako prepoznati prevarantske komentare?
- 5) Što je malvertising?

Motivacija

1. Psihološki trikovi i razna tehnologija za manipulaciju korisnicima
2. Potreban je razvoj boljih sigurnosnih protokola i edukacija korisnika
3. Podizanje svijesti

Social engineering [3]

- Napad društvenog inženjeringa je kibernetički napad koji se oslanja na psihološku manipulaciju ljudskog ponašanja kako bi se otkrili osjetljivi podaci, podijelile vjerodajnice, omogućio pristup osobnom uređaju ili na drugi način ugrozila digitalna sigurnost.

Vrste social engineering-a [4]

- Phishing
- Whaling
- Baiting
- Diversion theft
- Business Email Compromise (BEC)
- Smishing
- Quid Pro Quo
- Honeytrap
- Tailgating/Piggybacking

Scamming [1]

- Scamming na društvenim mrežama odnosi se na različite oblike prevara koje koriste platforme društvenih mreža za manipulaciju korisnicima, često putem lažnih profila, poruka ili ponuda, kako bi stekli osjetljive informacije, novac ili pristup računima.
- Phishing, smishing i honeytrap

Najpopularniji oblici scamming-a [1]

1. Lažne investicije
2. Lažne nagrade
3. Malvertising

Lažne investicije [1]

- komunikacija s prevarantima počinje od komentara na videima/objavama
- izbjegavanje postojećih mehanizama detekcije prevara
- lažno predstavljanje

Lažne investicije (2)

Komunikacija s prevarantima [1]

- Istraživanje Xigao Li-a, Amira Rahmatia i Nicka Nikiforakisa
- Investicija u kriptovalute i lažne nagrade
- Računi prevaranata aktivni od šest mjeseci

Kako prepoznati prevarantske komentare?

- Filter dizajn :
  - Tekstualni filter
  - Filter na temelju slike
  - Vremenski filter

Primjer iz stvarnog života

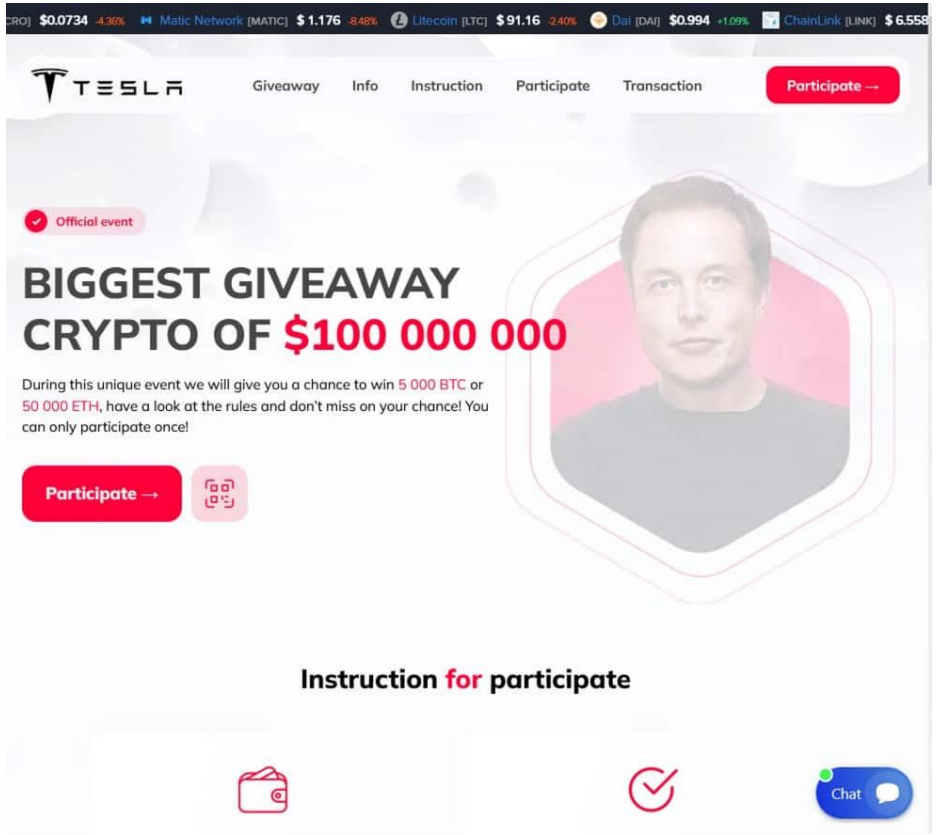
- Prodaja starog mobitela preko Njuškala
- Provođenje plaćanja putem zrcalne stranice DPD-a
- Bezuspješna prijava policiji

Lažne nagrade [2]

- 1) Izrada lažnog profila ili računa
- 2) Promocija lažnog "giveaway" događaja
- 3) Postavljanje uvjeta za sudjelovanje
- 4) Hitnost i ograničeno vrijeme
- 5) Imitiranje stvarnih događaja
- 6) Prikazivanje lažnih dokaza o isplati
- 7) Prijenosi uživo (Livestreams)
- 8) Nepovratna transakcija

Lažne nagrade (2)

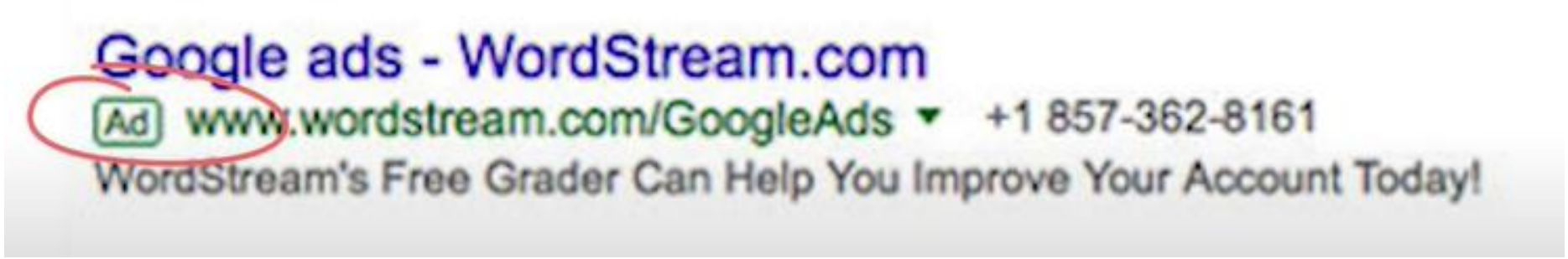
- Istraživanje James Lee-a, Emila K. Pucasa i Christa Wilsona



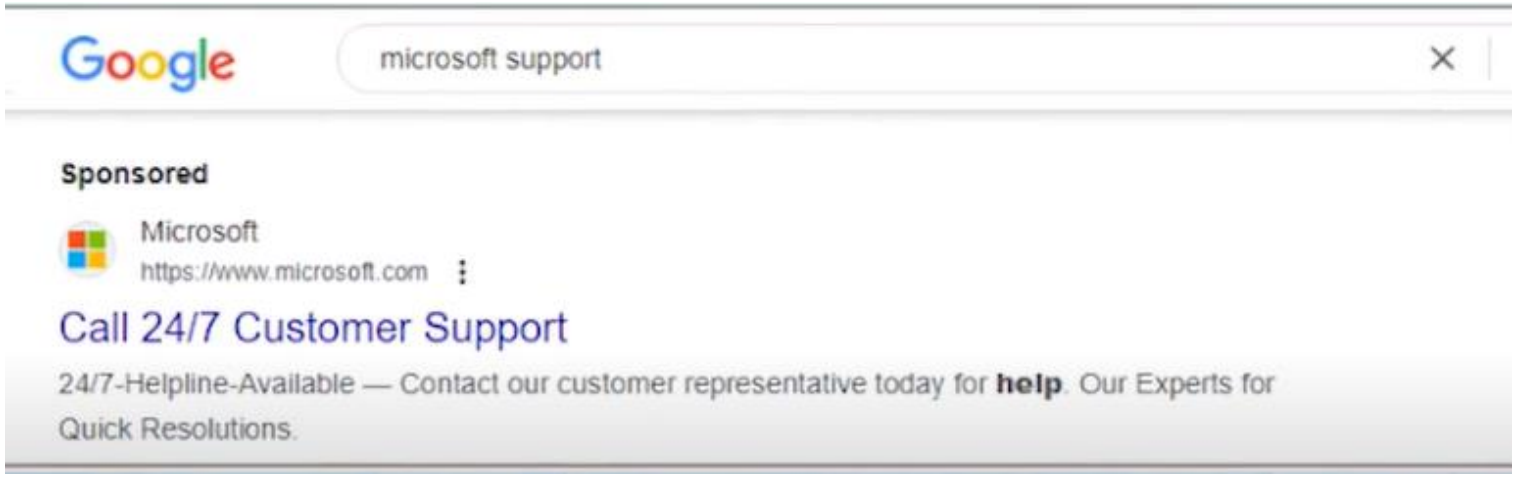
Malvertising [5]

- Praksa korištenja online oglasa za distribuciju malicioznih sadržaja, ali se može i shvatiti kao korištenje oglasa za manipulaciju korisnicima u svrhu plasiranje zlućudnih oglasa ili linkova.

Kako kriminalci dođu na vrh tražilice? [5]



Microsoftov incident [5]



Primjer iz pravog života (2)

- Kupnja tenisica putem lažne nike-ove stranice
- Dobivanje potvrdnog maila na engleskom jeziku
- Bezuspješna prijava policiji

Kako se zaštititi od prevara?

- Ne vjerovati ponudama koje zvuče jako dobro
- Upisivati podatke o kartici na provjerena mjesta (po mogućnosti koristiti prepaid kartice)
- Provjeriti URL stranice s koje kupujemo

Zaključak

- Treba aktivno razmišljati dok koristimo društvene mreže
- Prevaranti su postali sve domišljatiji
- Svatko može biti žrtva prevare

Literatura

- [1] Lenaerts-Bergmans, B. (2023, November 8). *10 types of social engineering attacks and how to prevent them*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/
- [2] Neupane, S., Mishra, A., Gopalan, S., Iliofotou, M., Jacobson, M., Krishnamurthy, A., Mao, Z. M., & Ramesh, M. (2023). *Automating the identification of giveaway scams on YouTube*. arXiv. https://arxiv.org/html/2405.09757v1
- [3] Kaspersky. (n.d.). What is social engineering? Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
- [4] INTERPOL. (n.d.). *Social engineering scams*. Interpol. https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams
- [5] YouTube. (2021, October 13). *Social engineering - how cybercriminals manipulate people*. [Video]. YouTube. https://www.youtube.com/watch?v=CPtFYk0bA-4
- [6] BBC News. (2016, August 23). Poor security 'aided' Ashley Madison hack. Retrieved from https://www.bbc.com/news/technology-37170542

Dodatna literatura

- Cloudflare. (n.d.). *What is a phishing attack?*. Cloudflare. https://www.cloudflare.com/learning/access-management/phishing-attack/
- Kaspersky. (n.d.). *What is a whaling attack?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack
- TerraNova Security. (n.d.). *What is baiting?* TerraNova Security. https://www.terranovasecurity.com/blog/what-is-baiting
- EasyDMARC. (n.d.). *What is diversion theft? Attack and defense strategies*. EasyDMARC. https://easydmarc.com/blog/what-is-diversion-theft-attack-and-defense-strategies/
- National Cyber Security Centre. (2020). *Business email compromise infographic*. Retrieved from https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf
- National Cyber Security Centre. (2020). Business email compromise infographic. Retrieved from https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf
- University of British Columbia. (n.d.). *Don't be fooled: Understanding the risks of quid pro quo cyber attacks*. Retrieved from https://privacymatters.ubc.ca/quid-pro-quo
- IBM. (2024, September 6). *What is pretexting?* Retrieved from https://www.ibm.com/topics/pretexting
- Yawar, S. (2024, August 31). *Honey trap in cyber security*. Pureversity. Retrieved from https://www.pureversity.com/blog/honey-trap-in-cyber-security
- Awati, R. (2022, August). *What is tailgating (piggybacking)?* TechTarget. Retrieved from https://www.techtarget.com/whatis/definition/tailgating-piggybacking
- Get Safe Online. (n.d.). *Get Safe Online: The UK's leading online safety advice resource*. Retrieved from https://www.getsafeonline.org/

Hvala!