Bachelor's thesis

Bachelor's Programme in Computer Science

A Novel Cybersecurity Threat: Artificial Intelligence in Social Engineering

Riku Talvisto

May 22, 2024

Faculty of Science

University of Helsinki

Contact information

P. O. Box 68 (Pietari Kalmin katu 5)
00014 University of Helsinki,Finland

Email address: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Study programme
Faculty of Science	Bachelor’s Programme in Computer Science

Tekijä — Författare — Author

Riku Talvisto

Työn nimi — Arbetets titel — Title

A Novel Cybersecurity Threat: Artificial Intelligence in Social Engineering

Ohjaajat — Handledare — Supervisors

Dr. Lea Kutvonen

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Bachelor’s thesis	May 22, 2024	7 pages

Tiivistelmä — Referat — Abstract

The integration of artificial intelligence (AI) into social engineering practices presents exceptional threats to privacy and security, necessitating a truly comprehensive re-evaluation, and enchantment, of current cybersecurity measures. Presenting both novel threats, as well as novel learning opportunities as countermeasures for AI attacks.

What, if anything, can the end user trust anymore?

ACM Computing Classification System (CCS)
General and reference → Document types → Surveys and overviews
Social and professional topics → Computing / technology policy → Computer crime
→ **Social engineering attacks**
Security and privacy → Intrusion/anomaly detection and malware mitigation
→ Social engineering attacks

Avainsanat — Nyckelord — Keywords

social engineering, artificial intelligence, cybersecurity, security, hacking, psychology

Säilytyspaikka — Förvaringsställe — Where deposited

Helsinki University Library

Muita tietoja — övriga uppgifter — Additional information

Contents

1 Introduction

Cybersecurity is

Social engineering is

In this article, we'll go through

How modern AI is

Finally, we'll conclude with some speculation about future AI-based attacks.

(Wang et al., 2020; Goossens et al., 1993; Knuth, 1999) Wang et al., 2020; Goossens et al., 1993; Knuth, 1999

2 Methods

It's crucial for any professional working in any industry to be aware of the different social engineering (SE) attacks. In this chapter, we'll go through the most common ones.

In a later chapter, we'll go through and analyze how modern AI augments these attacks, and how users of information systems need to be trained to counter these new, advanced threats.

As described by Abiteboul et al., 1997, the term *social engineering* is perhaps overused and is certainly misused. What exactly constitutes social engineering? In this paper, we'll use the defition of X by Y, "social engineering is the deliberate act of convincing a victim, usually though the use of technology, to perform an action that may or may not be in their best interest". Some have included acts like shoulder shurfing and dumpster diving as social engineering attacks, but since these do not rely on the manipulation of people we'll leave them outside the scope of this paper.

2.1 Phishing, Spear Phishing and Whailing

Phishing is the quintessial social engineering attack. It is characterized by malicious attemps to gain sensitive information from unsuspecting users, usually via email and by using spoofed websites that look like their authentic counterparts. Phishing has been around since 1996, when cybercriminals began using deceptive emails and websites to steal AOL (America Online) account information from unsuspecting users. However, the concept of tricking people goes a lot further than that, with people doing such deeds being called confidence men or "con artists".

Spear phishing is a more targeted version of phishing, where attackers customize their deceptive emails to a target individual or organization. Unlike with generic phishing attemps, this type of phishing involves gathering detailed information about the victim, such as their name, position and contacts to craft a convincing and personalized message. This tailored approach increases the likelyhood of the victim falling for the scam.

Last on our list of phishing attacks is **whaling**. Whaling, also known as CEO fraud, is a highly targeted phishing attack aimed at high-profile individuals within an organization, such as executives or senior management. The attackers carefly research their targets to create convinving and often urgent messages that appear to come from trusted sources, often impersonating colleagues, business partners, or government agencies. The goal is often to authorize large financial transactions or to leverage the target's authority and access within the company.

2.2 Pretexting

Pretexting, a term first used by FBI in YYY to descibe a situation where a fabricated story (a pretext) is used to lure

2.3 Tailgating

Tailgating refers to the act of "tailing" someone through a access-controlled passage, such as a security gate. The social engineer may hold something that looks heavy in their hands and ask for a person going in to let them through, thus bypassing the need to have a valid access authority

3 Results

4 Discussion

5 Conclusions

What's certain is that we can count on AI developing, AI-based social engineering attacks evolving with it, and the need for continuous, innovative user training growing in the future. Attackers and defenders are playing a never-ending game of "cat & mouse" where nobody can rest.

X in Y references that training users effects will wear off in 3 weeks, necessiting continous retraining approaches.

I'll end with the question that I started with; what, if anything, can the end-user trust anymore? And perhaps, with the advances in AI technology, the answer is "no-one".

Bibliography

Abiteboul, S., Quass, D., McHugh, J., Widom, J., and Wiener, J. (1997). “The Lorel query language for semistructured data”. In: *International Journal on Digital Libraries*, 1(1). [http://link.springer.de/link/service/journals/00799/bibs/7001001/70010068.htm, 18.1.2000], pp. 68–88.

Goossens, M., Mittelbach, F., and Samarin, A. (1993). *The LaTeX Companion*. Reading, Massachusetts: Addison-Wesley.

Knuth, D. E. (1999). *Digital Typography*. CLSI Lecture Notes (78). The Center for the Study of Language and Information.

Wang, Z., Sun, L., and Zhu, H. (2020). “Defining Social Engineering in Cybersecurity”. In: *IEEE Access*, 8. Conference Name: IEEE Access, pp. 85094–85115. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2992807. URL: https://ieeexplore.ieee.org/document/9087851 (visited on 11/15/2023).