Social engineering and phishing: A semiotic perspective

Nikola VANGELOV,
Associate professor, Faculty of Journalism and Mass Communication
Sofia University "St. Kliment Ohridski", Sofia, Bulgaria
nlvangelov@uni-sofia.bg

Abstract

This paper examines social engineering and phishing through the analytical lens of semiotics, with the purpose of uncovering how deceptive digital messages manipulate signs and symbols to influence perception and behavior. The primary goal is to provide a deeper understanding of the communicative techniques that underlie phishing attacks by analyzing how attackers mimic trusted entities, exploit cognitive shortcuts, and manipulate emotional and contextual cues. Using qualitative semiotic analysis, the paper dissects real-world phishing examples—such as fraudulent emails, fake login pages, and spoofed interfaces—to identify the semiotic mechanisms at play. The study is organized around three thematic areas: the construction of deceptive signs and symbols, exploitation of perceptual shortcuts and imitation of interface iconography. By situating phishing within a semiotic framework, the paper aims not only to expose the techniques used by malicious actors but also to suggest strategies for what can be termed "defensive semiotics"—design and educational approaches that enhance users' critical interpretation of digital signs. In doing so, this research contributes to a more nuanced understanding of digital deception and the symbolic construction of trust online.

Keywords: semiotics, online security, cognitive shortcuts, deceptive interfaces, defensive semiotics.

1. Introduction: Framing social engineering and phishing through semiotics

In an era where digital communication permeates every facet of daily life, the manipulation of perception and behavior through subtle cues and messages has become both more sophisticated and more dangerous. Phishing attacks—fraudulent attempts to obtain sensitive information by disguising as trustworthy entities—have evolved into a significant threat in the cybersecurity landscape. At their core, these attacks are not merely technical exploits; they are symbolic manipulations. To fully grasp their power, we must turn to a field that specializes in the study of signs, symbols, and meaning: semiotics.

The global proliferation of digital devices has dramatically increased the avenues through which social engineering attacks operate. As of 2024, there are approximately 6.8 billion smartphone users worldwide, representing over 85% of the global population [1]. Additionally, over 5 billion people have access to the internet, with most interacting through multiple digital devices including laptops, tablets, and smart home technologies [2]. This vast and interconnected digital ecosystem provides fertile ground for attackers who exploit trust embedded in semiotic systems such as logos, email formats, website layouts, and even social media cues.

Semiotics, the study of signs and the processes by which meaning is constructed and understood, offers a rich conceptual framework for analyzing phishing and other forms of social engineering. Originating in the works of Ferdinand de Saussure [3] and Charles Sanders Peirce [4], and later expanded by theorists such as Roland Barthes [5] and Umberto Eco [6], semiotics helps unpack how individuals interpret signs—be they words, images, sounds, or even user interface elements. In the context of phishing, attackers weaponize signs to trigger trust, urgency, or fear, guiding users toward compromising actions.

Social engineering, broadly defined as the psychological manipulation of individuals into performing actions or divulging confidential information, thrives in digital environments where identity and trust are mediated through symbolic representations. According to Ardjomandi, in phishing, attackers often impersonate legitimate entities by mimicking visual, linguistic, and structural signs—company logos, email formats, domain names, and user interfaces—crafted to deceive recipients [7]. Zankova believes that trust, unlike physical trust, relies heavily on the recognition and interpretation of these semiotic cues [8]. The same applies to smart cities [9].

Recent studies underscore the scale and impact of phishing attacks. For example, the Anti-Phishing Working Group (APWG) reported over 270,000 unique phishing sites detected in the third quarter of 2023 alone, marking a 15% increase from the previous year [10]. This surge is attributed to the attackers' increasing sophistication in semiotic mimicry, which enhances their ability to manipulate users' perceptions and behaviors.

This paper proposes that a semiotic lens is not only appropriate but crucial for understanding the underlying dynamics of phishing. By asking, *How do attackers use signs and symbols to manipulate perception and behavior?*, we open a path to a deeper analysis of both the mechanics of deception and the means of defense. A semiotic approach can illuminate the hidden logic of trust in digital communication—and help us design better strategies to resist manipulation [11], [7].

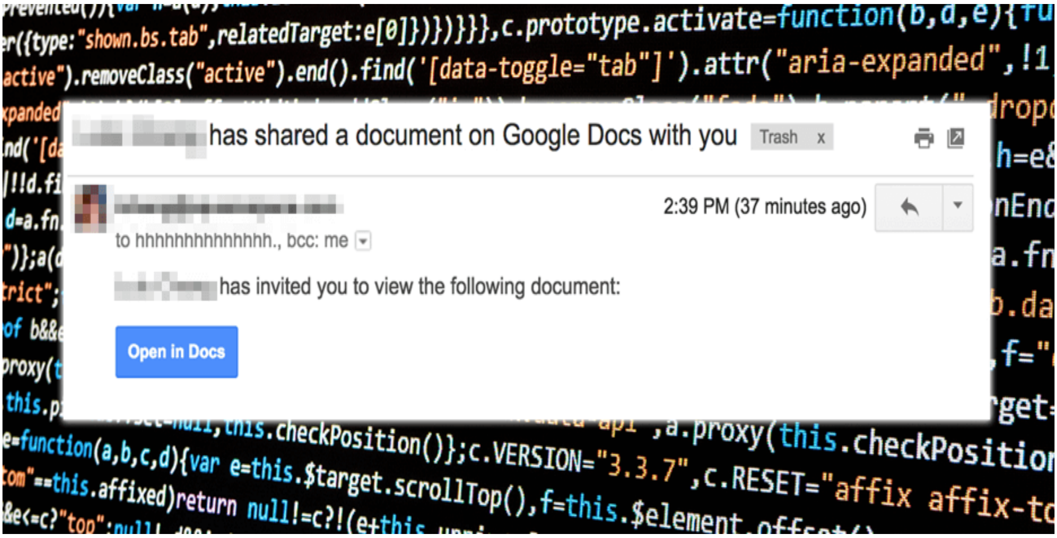
2. Crafting deceptive signs and symbols

In semiotics, the study of signs and symbols as elements of communicative behavior, Ferdinand de Saussure conceptualized the sign as composed of two parts: the signifier (the form which the sign takes) and the signified (the concept it represents) [3] . When a social engineer crafts a phishing message, they deliberately manipulate these components to create deceptive signs that mimic trusted entities, triggering recognition and trust in the recipient's mind. Charles Sanders Peirce's triadic model further enriches this understanding by emphasizing the representamen (the form of the sign), the object (what the sign refers to), and the interpretant (the meaning derived by the receiver) [4]. Attackers exploit this interpretant by triggering the user's learned associations with familiar symbols, such as corporate logos or email templates.

Roland Barthes extended semiotic theory by highlighting mythologies, or cultural connotations attached to signs beyond their literal meaning [12]. For instance, a company logo is not just a graphic but carries cultural weight as a symbol of legitimacy, security, and authority. Phishers leverage this mythological layer to craft deceptive messages that feel authentic, exploiting users' semiotic literacy gaps.

Real-world example: The Google docs phishing scam (2017)

In 2017, a widespread phishing campaign exploited these semiotic principles by sending emails that appeared to be Google Docs invitations from trusted contacts (figure 1). The emails employed Google's branding and a familiar interface design to signal authenticity (signifier), while the concept signified was access to a shared document. However, the underlying object was malicious: a fake app requesting unauthorized permissions.



[redacted] has shared a document on Google Docs with you

[redacted] 2:39 PM (37 minutes ago)

to hhhhhhhhhhhhhh., bcc: me

[redacted] has invited you to view the following document:

Fig. 1 The Google Docs Phishing Scam (2017)

Despite subtle differences—such as the name of the requesting app—the crafted signs effectively exploited users' trust [13]. The linguistic simplicity and generic phrasing further obfuscated the message's deceptive nature, relying on the recipient's assumption that a Google Doc invite is safe. The same principle applies to some social media channels [14].

Visual Breakdown

- **Logo and Branding:** The phishing email included Google's recognizable logo and color scheme, which served as powerful signifiers. Minor anomalies, like unusual spacing or slightly altered colors, were often overlooked due to cognitive biases toward familiar signs.
- **App Name:** The malicious app was labeled "Google Docs" but was actually a different entity requesting access permissions. This signifier was critical because users often do not inspect app names carefully.
- **Email Address:** The sender appeared as a known contact, leveraging the recipient's trust network to strengthen the interpretant—meaning users interpreted the message as safe due to familiar sender signs.
- **Language Use:** The email's language was intentionally generic, lacking the more formal tone typical of Google's official communications, but this difference was subtle enough not to raise immediate suspicion.

Table 1. Visual Breakdown of the Google Docs Phishing Scam

Element	Legitimate Google Docs Invite	Phishing Google Docs Scam	Semiotic Note
Sender Email	user@trustedcontact.com	user@trustedcontact.com (spoofed or hacked)	Familiar sender address increases trust (interpretant).
Subject Line	“[Name] has shared a Google Doc with you”	“[Name] has shared a Google Doc with you”	Identical phrasing leverages familiarity (signifier).
Logo and Branding	Google’s official logo with exact colors	Google’s logo, colors slightly off or pixelated	Familiar symbol triggers recognition despite minor flaws.
Email Body Text	Formal, precise language, personalized greeting	Generic, simple language, no personalization	Lacks typical personalization, which is a subtle warning sign.
Link Destination	accounts.google.com/document/...	phishing-domain.com/google-docs/...	URL visually close but different; critical signifier for trust.
App Permission Name	Google Docs	“Google Docs” (fake app requesting access)	The app name is the signifier of the malicious intent.
Visual Layout	Clean, consistent formatting	Slight irregularities in spacing or font	Minor formatting anomalies often overlooked due to trust bias.

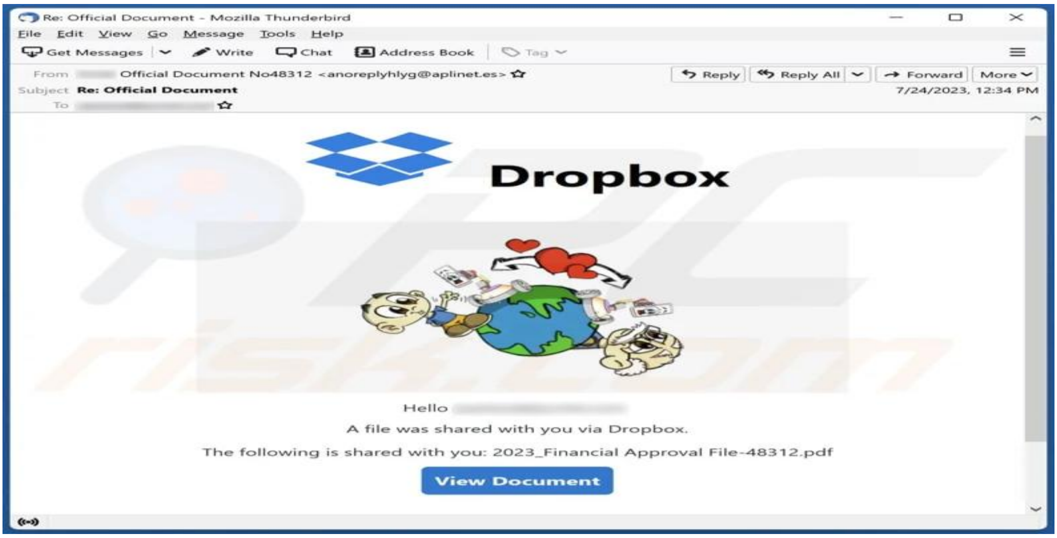
3. Exploiting semiotic shortcuts

Human beings are efficient processors of visual and linguistic information, often relying on cognitive shortcuts—or what semiotics would describe as *abbreviated readings* of signs [12]. According to Charles Sanders Peirce, a sign consists of three interrelated components: the *representamen* (the form), the *object* (what it refers to), and the *interpretant* (the effect or meaning it generates) [4]. In the digital environment, attackers exploit the *interpretant* by designing stimuli that visually resemble legitimate signs, banking on the user’s conditioned response to symbols like domain names, logos, and familiar interface layouts.

Similarly, Saussure’s dyadic model of the *signifier* (the form of the sign) and *signified* (the concept it represents) helps us understand how phishing attacks manipulate perception by creating deceptive alignments between visual cues and expected meaning [3]. These manipulated signs bypass deeper cognitive processing and trigger automatic, habitual responses.

Real-world example: Dropbox file share scam

In this case [15], attackers sent emails claiming a colleague had shared an important file through Dropbox (figure 2). The message contained a link leading to a fake Dropbox login page. This counterfeit page replicated Dropbox’s visual language—including its color scheme, typography, and layout—with minor inconsistencies. The sender’s email address and the URL (e.g., "dropbox-files.com") were intentionally similar to the legitimate "dropbox.com" domain, exploiting what Peirce might call an *iconic* resemblance to legitimate interfaces.



Re: Official Document - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More

From [redacted] Official Document No48312 <anoreplyhlyg@aplinet.es>

Subject Re: Official Document

To [redacted]

7/24/2023, 12:34 PM

Dropbox

Hello [redacted]

A file was shared with you via Dropbox.

The following is shared with you: 2023_Financial Approval File-48312.pdf

Fig. 2: How to avoid falling for scams like "A File Was Shared With You Via Dropbox"

The linguistic register of the email was another key element. It used overly formal phrasing—“You have received the important document. Please open it immediately for reviewing”—which subtly deviated from Dropbox’s typically concise and casual tone. Despite these minor anomalies, the interplay of familiar visual and verbal signs created a *myth* of authenticity in the Barthesian sense: a culturally coded assumption of trustworthiness attached to the Dropbox brand [12].

Visual Breakdown

- **Email Layout:**
  - Logo at the top using Dropbox’s standard blue and white color scheme.
  - Formal message such as “A file has been shared with you.”
- **Hyperlink:**
  - A button labeled "View File" directed users to a nearly identical login page.
  - The link, when hovered over, revealed a deceptive domain such as “dropbox-files.com.”
- **Sender’s Email:**
  - Seemingly legitimate, but actually from “alerts@dropboxnotify.com” instead of “dropbox.com.”
- **Linguistic Markers:**
  - Unnatural phrasing and lack of personalization (e.g., “Dear User”).
  - A subtle urgency in tone, prompting users to act quickly.

Table 2

Element	Legitimate Dropbox	Phishing Page	Semiotic Manipulation
Logo	Authentic Dropbox logo with consistent proportions	Slightly altered or pixelated logo	Exploits iconic similarity (Peirce); user assumes legitimacy based on visual resemblance
Color Scheme	Standard blue and white branding	Near-identical but may use slightly off shades	Mimics brand identity to trigger recognition heuristics
URL / Domain Name	https://www.dropbox.com/	http://dropbox-files.com/ or drop-boxlogin.com	Relies on orthographic ambiguity (e.g., added hyphen, fake TLD)
Sender Email Address	alerts@dropbox.com or no-reply@dropbox.com	alerts@dropboxnotify.com or files@dropbox-mail.net	Fakes institutional authority through domain mimicry
Greeting & Tone	Personalized and concise: "Hi John, here's your file."	Generic and formal: "Dear User, you have received the important file"	Uses non-personalization and anomalous tone—semiotic clues of inauthenticity
Button / CTA	"View File" or "Open" with secure hover URL	Same label, but hover reveals unsecure or misleading URL	CTA is a symbol of trust—manipulated to mislead
Security Indicators	HTTPS lock icon, proper certificate	Lock icon may be present visually but not functionally (no HTTPS)	False security cues mislead the interpretant into assuming safety

These semiotic cues collectively guided users toward an *incorrect interpretant*—one that perceived legitimacy where there was none. By exploiting visual and syntactic shortcuts, attackers triggered a recognition heuristic that bypassed critical scrutiny.

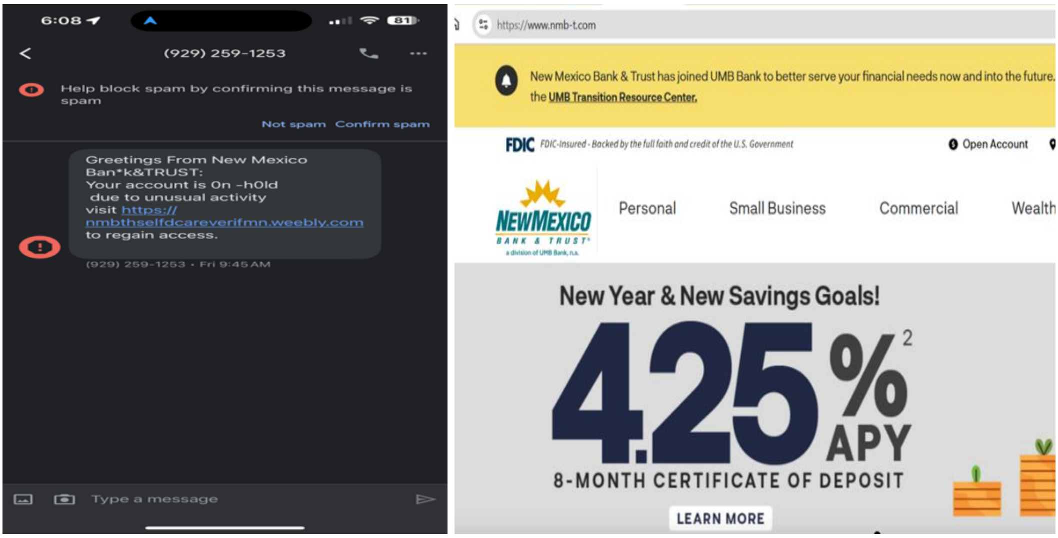
4. Manipulating context and connotation

Semiotics isn't only about literal interpretation—it's also about *connotation*, or the associative meanings that signs evoke [12]. While *denotation* refers to the literal meaning of a sign (e.g., a word like "locked"), connotation involves cultural and emotional overlays—"locked" connotes urgency, danger, or exclusion, depending on the context. In phishing, these connotative cues are deliberately used to trigger emotional responses such as anxiety, fear, or haste, pushing users to act without reflection.

Peirce's *indexical signs*—those that point toward a cause or consequence—are especially relevant here. A message claiming "suspicious activity" on a bank account functions as an indexical sign of danger. Combined with symbolic signs (like a bank logo) and urgent language, these cues manipulate user behavior through emotionally charged semiotic constructs.

Real-world example: Fake banking website via SMS (Smishing)

In this scenario, users receive a **text message** claiming there is urgent activity on their bank account and instructing them to click a link to "verify" or "secure" their account (figure 3a and 3b). The link opens a **fraudulent mobile banking website** that mimics the real one but includes subtle discrepancies—such as unusual domain names (banking.c0m with a zero instead of an "o"), generic greetings, and altered typography.



Help block spam by confirming this message is spam

Greetings From New Mexico Ban*k&TRUST:
Your account is On -hOld
due to unusual activity
visit https://nmbthselfdcareverifmn.weebly.com
to regain access.

(929) 259-1253 • Fri 9:45 AM

New Mexico Bank & Trust has joined UMB Bank to better serve your financial needs now and into the future. the UMB Transition Resource Center.

FDIC
FDIC-Insured - Backed by the full faith and credit of the U.S. Government
Open Account
NEWMEXICO
BANK & TRUST
a division of UMB Bank, n.a.
Personal
Small Business
Commercial
Wealth
New Year & New Savings Goals!
4.25%
2
APY
8-MONTH CERTIFICATE OF DEPOSIT
LEARN MORE

Fig. 3a and 3b: Catch Of The Week: NMB&T Themed Smishing Scams

The semiotic strategy here is clear: attackers weaponize the indexical sign of the SMS alert, using words like “suspicious,” “urgent,” or “locked” to invoke emotional connotations that override rational decision-making. By placing the user in a simulated crisis, the phisher manipulates interpretation through carefully chosen signs that “mean more” than they say.

🔍 Table 3. Visual Breakdown: Fake Banking Website (Smishing)

Element	**Legitimate Banking Site**	**Phishing Page**	**Semiotic Manipulation**
Sender ID (SMS)	“YourBank” or short code verified sender	“BankSecure” or spoofed number	Symbolic authority in sender name gives message credibility
Message Content	"Unusual login detected. Visit your account to confirm."	"Suspicious activity detected. Click here to avoid account lock."	Language conveys indexical threat and triggers connotative urgency
URL / Domain	https://yourbank.com	http://yourbánk.com or yourbank-alerts.net	Uses homoglyphs (e.g., accented characters, fake TLDs) to mislead
Greeting & Tone	"Dear John, please verify recent login."	"Dear Customer, we noticed suspicious activity."	Lack of personalization signals inauthenticity, but users often miss it under stress
Page Layout	Responsive, minimal, HTTPS secure	Close mimic, lacks SSL or uses outdated UI elements	Visual mimicry reinforces iconic similarity but with subtle inconsistencies
Security Indicators	Padlock icon, valid certificate	Fake padlock icon or no SSL at all	Visual symbol of security is faked—false trust cue

This scam illustrates how digital deception often occurs not just at the level of **what is shown**, but **how it is framed**. The emotional environment—created by urgent language and manipulated context—is as essential as the signs themselves.

5. Discussion

This paper has shown that social engineering and phishing are not merely technical issues but deeply semiotic phenomena. Through deceptive use of signs—logos, language, layout, and symbols—phishers exploit the ways humans interpret and assign meaning. As Barthes [5] famously noted, signs are not neutral; they carry layers of denotation and connotation that shape perception. In phishing attacks, both levels are manipulated to bypass rational scrutiny.

Each real-world case study highlights how attackers deploy semiotic strategies:

- In the *Google Docs scam*, the sign of a trusted Google logo functioned as an index of legitimacy, triggering trust based on past interaction.
- The *Dropbox scam* exploited the heuristic recognition of branding and domains, a cognitive shortcut that Peirce [4] would classify as a form of habitual interpretant—a learned pattern that the user assumes to be trustworthy.
- The *Fake Banking Website* leveraged iconography like padlocks and corporate color schemes to construct an illusion of security, suggesting that trust in digital environments is heavily dependent on visual codes rather than verified content [3].

This use of signs shows that phishers understand, intuitively or explicitly, how digital trust is built semiotically. They weaponize design, tone, typography, and even grammar to simulate legitimate communication. Saussure's concept of the arbitrariness of the sign is especially relevant [3]: a padlock symbol has no inherent connection to security—its meaning is socially constructed. Once that cultural association is established, it can be hijacked.

More critically, phishing succeeds not only by imitation but also by speed and emotional manipulation. The connotative power of words like "urgent," "locked," or "verify" activates emotional responses (fear, anxiety, curiosity), suppressing critical evaluation. This underscores a vital point: semiotic literacy is as essential as digital literacy in the fight against phishing [16], [17].

The discussion also raises a deeper implication: our increasingly digital world requires new cognitive defenses. As users move seamlessly between interfaces, brands, and platforms, they often do not pause to interrogate signs. This leaves space for manipulation. Without a conscious awareness of semiotic structures, users are vulnerable to deception that operates below the threshold of attention.

Defensive semiotics offers a promising framework to mitigate these risks by cultivating an awareness of signs and encouraging critical scrutiny of digital communication. Users can be trained to identify subtle inconsistencies in visual and linguistic signs that signal phishing attempts, such as minor deviations in logos, suspicious domain names, or atypical phrasing. Such education empowers users to move beyond superficial recognition and engage in analytical reading of digital messages. As Barthes [5] emphasized, understanding the connotative layers of signs helps reveal their underlying messages and manipulations. Bødker and his colleagues believe that practical exercises in semiotic anomaly detection could be integrated into cybersecurity awareness programs to enhance users' ability to spot deception before harm occurs [18].

Organizations also have a critical role in designing communication that is inherently harder to mimic. This can involve developing unique, dynamic semiotic markers—such as personalized digital signatures, multi-factor visual cues, or adaptive language patterns—that attackers find difficult to replicate convincingly. Saussure's notion of the arbitrary sign suggests that while signs are socially constructed, their complexity and uniqueness can be leveraged defensively [3]. For example, according to Miami University IT services [19], encrypted QR codes or interactive authentication steps embedded in emails can serve as semiotic "watermarks" that confirm legitimacy.

Finally, semiotic literacy should be integrated as a fundamental component of digital literacy and cybersecurity education. Beyond teaching technical skills, programs must emphasize how meaning is constructed and communicated in digital environments. This aligns with calls to expand digital literacy to include interpretive and critical thinking abilities [17]. By understanding the semiotic processes at play, users develop a meta-awareness that strengthens their overall resilience against manipulation, fostering a more informed, cautious, and empowered user base.

6. Conclusion

This study has demonstrated that phishing and social engineering are fundamentally semiotic phenomena, relying on the strategic manipulation of signs and symbols to deceive users and exploit trust. By applying semiotic theory, including the foundational work of Saussure, Peirce, and Barthes, we gain a clearer understanding of how attackers craft messages that appear legitimate through visual, linguistic, and contextual cues. The real-world examples examined show how seemingly minor semiotic shifts—such as altered logos, domain names, or phrasing—can create convincing illusions that bypass users' critical faculties.

Moreover, the analysis highlights that phishing attacks do not simply rely on imitation but also on emotional triggers and cognitive shortcuts embedded in semiotic processes. This underscores the urgency of incorporating semiotic literacy into broader digital literacy and cybersecurity education. Users trained to recognize semiotic anomalies and understand the layered meanings of digital signs will be better equipped to resist manipulation.

Organizations must also embrace semiotic strategies defensively, designing communication that is more complex and dynamic to thwart mimicry by attackers. This dual approach—educating users and innovating communication design—can reduce the efficacy of phishing campaigns and enhance digital trust.

Finally, as digital environments evolve, so too must our frameworks for understanding and combating deception. Future research should explore the semiotics of emerging threats, such as AI-generated phishing content and cross-cultural semiotic variations in scams, to develop more sophisticated defensive tools. Overall, this semiotic perspective opens new pathways for strengthening cybersecurity by emphasizing the interpretive and symbolic dimensions of digital communication.

References

[1] Statista, „Number of smartphone mobile network subscriptions worldwide from 2016 to 2025, with forecasts from 2025 to 2028," [Онлайн]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Отваряно на 27 05 2025].

[2] Internet World Stats, „Internet usage statistics," 2024. [Онлайн]. Available: https://www.internetworldstats.com/. [Отваряно на 24 05 2025].

[3] F. Saussure, Course in general linguistics, New York: Philosophical Library, 1959.

[4] C. S. Peirce, „The Collected Papers of Charles Sanders Peirce," в *C. Hartshorne, P. Weiss, and A. W. Burks, Eds.,* Harvard University Press, p. 1931–1958.

[5] R. Barthes, Mythologies, New York : The Noonday press, 1972.

[6] U. Eco, A theory of semiotics, Bloomington: Indiana University Press, 1976.

[7] A. Ardjomandi, „Visual Semiotics and User Perception in Digital Interface Design," *IRE Journals* , том 8, № 10, 2025.

[8] B. Zankova, „Smart citizens for Smart cities: the role of social media for expanding local democracy (The case of local referendums in Bulgaria)," *Smart Cities and Regional Development,* том 2, № 2, pp. 19-33, 2018.

[9] C. Vrabie, „Smart Urban Governance. Administrația Publică în era Smart: Tehnologie, Date și Cetățeni," *Smart Cities and Regional Development,* том 1, № 1, 2024.

[10] Anti-Phishing Working Group, „Phishing Activity Trends Report, Q3-2023," 2023. [Онлайн]. Available: https://apwg.org/trendsreports/. [Отваряно на 28 05 2025].

[11] B. Zankova , „Smart society – "Fake analytica" style?," *Smart Cities and Regional Development,* том 3, № 1, 2019.

[12] R. Barthes, Image, Music, Text, Great Britain: FontanaPress , 1977.

[13] Office of the Comptroller of the Currency, „Fraud Resources. OCC Consumer Advisory," 2023. [Онлайн]. Available: https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html.

[14] A. F. Rahmat, C. Vrabie и G. B. Soesilo, „Exploring the Cybercrime Prevention Campaign on Twitter: Evidence from the Indonesian Government," *Smart Cities and Regional Development,* том 7, № 2, p. 9–24, 2023.

[15] J. McDonald, „Phishing Examples: Google Docs Scam," 2017. [Онлайн]. Available: https://www.compassitc.com/blog/phishing-examples-google-docs-scam. [Отваряно на 24 05 2025].

[16] D. Chandler, Semiotics, The basics, Second edition, том 2, 2007.

[17] K. Parsons, M. Butavicius, M. Pattinson, D. Calic, A. Mccormac и C. Jerram, „Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?," *Computer Science > Computers and Society, arxiv* , 2016.

[18] H. Aldawood и G. Skinner, „Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet* , том 11, № 3, 2019.

[19] Miami University IT Services, „Recent phishing scams: Google Docs and QR codes," 2024. [Онлайн]. Available: https://miamioh.edu/it-services/news/2024/05/phishing-scams-may24.html. [Отваряно на 06 05 2025].