Evaluating the Effectiveness of Short Video Advertisements in Fostering Virtual Identity Security Awareness Among Youth

Shimaa Salah Sadek Sedek [1*]

1 Associate professor, Advertising department, faculty of applied arts, Benha University, Qalyubia, Egypt.

Submit Date: 2024-03-14 21:51:05 | Revise Date:2024-07-15 13: 10:22 | Accept Date: 2024-07-16 12: 16:09

DOI: 10.21608/jdsaa.2024.277007.1404

KEYWORDS:
Short Video Advertisements, Virtual Identity, Security Awareness, Identity Theft, Awareness Advertisements.

ABSTRACT:

The research addresses the issue of insecure internet use among young people, leading to heightened concerns about potential theft of users' virtual identities and the propagation of cyber-attacks. The study purposes to increase awareness for young users about the consequences associated with virtual identity theft. It also aims to promoting a secure use to personal identity management in their digital world. Additionally, the study goes beyond mere awareness and explores the effect of short video ads on behavioral changes among young users. The significance of this study stems in its potential to address a pressing societal issue. With the increasing rate of internet usage among youth and the rise in cyber threats such as identity theft. The study employed an experimental method to test hypotheses by creating three short video advertisements aimed at raising awareness of virtual identity security. The research results uncover significant findings. Particularly, statistically meaningful variances were identified in the mean scores of responses among youth participants prior to and following exposure to short advertisements targeting the promotion of virtual identity security awareness. Furthermore, a discernible alteration in their online practices pertaining to virtual identity security was observed.

1- Introduction

In the digital age, virtual identity theft stands out as a prevalent and severe crime, involving the unlawful acquisition and misuse of individuals' personal information. This illicit activity commonly targets sensitive data, such as internet usernames, passwords, financial particulars, and other personally identifiable information, intending to impersonate users for fraudulent purposes. Consequently, individuals become vulnerable to theft and fraud orchestrated by cybercriminals.

Crimes associated with identity have emerged as a major and escalating issue over the past two decades, primarily attributed to the considerable economic damage inflicted on victims. The heightened prevalence and accessibility of personal information online have substantially elevated the threat of identity-related fraud. However, there has been limited exploration into the factors influencing the probability of falling victim to this type of crime (Holt & Turner:2012).

The repercussions of such attacks are substantial, encompassing the unauthorized acquisition and misuse of users' personal information, leading to potential losses like harm to one's reputation, financial damage, and involvement in forgery and fraudulent activities. This, in turn, exposes users to potential legal consequences. Consequently, virtual identity theft presents extensive consequences and poses challenges in recovering stolen virtual identities.

The research addresses the issue of insecure internet use among young people, leading to heightened concerns about potential theft of users' virtual identities and the propagation of cyber-attacks. Despite this, a gap exists in understanding the effectiveness of short video ads in improve awareness and behavioral changes for users adopting a secure use to virtual identity. The study purposes to increase awareness for young users about the consequences associated with virtual identity theft. It also aims to foster a enhance virtual identity protection, promoting a secure use to personal identity management & information in their digital world. The research seeks to evaluate the effectiveness of short video ads in enhancing awareness for young users regarding the importance of virtual identity security, encouraging safe behavior for online use, and promoting secure management of virtual identities. Additionally, the study goes beyond mere awareness and explores the effect of short video advertisements on behavioral changes among young users concerning virtual identity security.

This study specifically focuses youth due to their heightened susceptibility to online threats stemming from their limited knowledge regarding internet security measures. Oftentimes, youth may engage in risky online behaviors without fully understanding the potential ramifications. Additionally, given their substantial internet usage for socializing, entertainment, and other purposes, youth represent a significant demographic in online spaces. Therefore, gaining insights into their behaviors and attitudes towards virtual identity security is necessary for devising effective awareness campaigns. The significance of this study stems in its potential to address a pressing societal issue. With the increasing rate of internet usage among youth and the rise in cyber threats such as identity theft, there is a serious need to explore innovative awareness campaigns for raising and promoting safe online behaviors. This research has the potential to enhance the internet safety initiatives and helping to mitigate the risks associated with online activities for young individuals.

The study employed an experimental method to test hypotheses by creating three short video advertisements aimed at raising awareness of virtual identity security. The study utilized a questionnaire adapted from Kruger and Kearney

(2006), administered both before and after the presentation of these short video ads on YouTube to assess their impact on Egyptian youth. The research proposes three hypotheses:

- There are statistically significant differences between the mean scores of the responses of the youth sample before and after exposure to short advertisements aimed at promoting awareness of virtual identity security among youth.

- There are statistically significant differences at a significance level (≥ 0.05) between the mean scores of responses from the sample of youth before and after exposure to short advertisements aimed at enhancing behavioral changes self-reported regarding virtual identity security among young people.

- There are statistically significant differences between the mean scores of responses from the youth sample before and after exposure to short advertisements, indicating a shift from merely increasing awareness to actual behavioral changes in online practices related to virtual identity security.

2- Theoretical background

3- The Nature of Virtual Worlds

The commonness of electronic commerce and financial services that enable access to user personal data, such as bank records and financial data have significantly increased the chances offenders have to engage in high tech identity fraud (see Allison et al. 2005; Chu et al. 2010; Furnell 2002; Holt and Lampke 2010; Newman and Clarke 2003; Wall 2007). Businesses institutions store user personal & sensitive information in huge electronic databases that can be retrieved by hackers (Chu et al. 2010; Holt and Lampke 2010; Newman and Clarke 2003; Wall 2007). For example, businesses reported losses of $500,000 in 2008 due to financial fraud incidents (Computer Security Institute 2009), while individual consumers lost an average of $575 to numerous types of on-line fraud in 2009 (Internet Crime Complaint Center 2010). In adding, the TJX Corporation recently reported that hackers compromised an internal database and stole at least 94 million user credit card accounts, and financial agencies approximation this will cause as much as $1 billion dollars in damages (Goodin 2007).

People who fall prey to various forms of cybercrime may find themselves at a higher risk of identity theft. For instance, individuals who are targeted by online harassment often report incidents where their perpetrators hijack their identities, disrupting or influencing their activities (Finn 2004; Holt and Bossler 2009). Given that many sophisticated identity thieves in the digital realm employ malicious software to compromise computer systems or steal sensitive information (Chu et al. 2010; Holt and Lampke 2010; Morris 2010), it's plausible that those whose computers are infected with malware face an elevated risk of becoming victims themselves.

4- Virtual Identity theft Meaning

ID theft, according to Mercuri (2006), is described as the unauthorized utilization of an individual's identity, conducted without their awareness, involving the transfer or use of information for criminal activities, which is deemed illegal under the law (Jougleux 2012). Identity theft is committed by phishing, by using an e-mail without the authorization of his owner and by using the name of others in a social network, etc. The various forms of identity theft led to different legal responses, according to the legal system of the country which is competent to regulate the issue and to the nature of the acts (Eszteri & Máté:2016)

Cole and Pontell (2006) provided valuable insights indicating that cybercrime and identity theft-related frauds are rapidly increasing worldwide. Although the situation is recognized as a global phenomenon affecting economies universally, assessing the damages proves to be a challenging and intricate task. The repercussions of cybercrime and identity theft extend far beyond what can be easily calculated or comprehended, as highlighted by Allison et al. (2005). In the contemporary era, both individuals and organizations must exercise caution when revealing their identities to safeguard against identity theft. In 2008, a Federal Trade Commission report revealed that approximately 9.9 million individuals experienced incidents of identity theft (Mugari et.al 2016: Gupta 2020).

While there is an increasing body of literature that observes trends, patterns, and emerging techniques related to identity theft, along with insights into the general traits of victims and factors contributing to the risk of identity theft, there is a scarcity of knowledge associated with the consequences of identity theft (Irvin-Erickson & Ricks, 2019; Piquero et al., 2011).

5- Causes Contributing to Identity Theft

- **Political**: Political and economic factors play a significant role in the rise of identity theft. Instances of ID theft often escalate during periods of economic and political instability in developing nations. Each year, millions of individuals from developing or underdeveloped countries migrate to developed countries, either through legal or illegal means (UNHCR, 2007).

- **Social**: In the realm of social factors contributing to identity theft, habits and communication methods are crucial elements. The literacy rate within an economy awareness of the use of social networking sites are key factors in privacy in the virtual environment. Various measures are implemented by organizations to safeguard their confidential data and uphold privacy. According to Applegate (2009), social engineering is systematically employed by thieves to exploit organizational systems through identified vulnerabilities, specifically targeting the human factor within the organization. With the prevalent trend of increased usage of social networking sites compared to real-world interactions, individuals become more susceptible to identity theft.

- **Technological factors**: if individuals and originations fail to adopt proper secure ways, they will be exposed to significant risks. It's important to acknowledge that sharing personal information online is not secure. The Internet, often considered a treasure for cybercriminals, it's an easy access to information and leads to annual losses of nearly $40 billion. (Chander Mohan Gupta and Devesh Kumar: 2020)

6- Key Components of Virtual Identity

- Digital Persona Creation: Establishing a virtual identity involves purposefully crafting a digital persona that reflects individuals wanted online image. This process is shaped by personal choices, societal expectations, and the distinctive characteristics of the platform being used. (Subrahmanyam & Šmahel 2010)

- Curated Self-Representation: People frequently shape their virtual identities by deciding which facets of their lives to reveal online. This thoughtful selection in self-presentation provides a measure of effect over how others perceive them. (Subrahmanyam & Šmahel 2010)

- Flexibility & Adaptability: Virtual identity is inherently supple, providing individuals with the opportunity to experiment with different facets of their personality, affiliations & interests. This adaptability permits for a more nuanced appearance of oneself.

- Digital Track: Each online interaction contributes to a digital trail, founding a comprehensive form of an individual's virtual activities. This trail significantly influences user's online personality and shapes how audiences perceive them.

- Identity Examination: Online spaces proposal a unique environment for users to explore features of their identity that might not be as openly expressed in their real lives. This exploration contributes to self-discovery.

- Anonymous & Pseudonymous Interaction: The digital world allows for variable degrees of anonymity, enabling users to engage without revealing their real identities. While this can foster open, it also increases accountability concerns.

- Privacy: Managing virtual identity includes navigating complex privacy and security considerations. Protecting personal information is crucial for maintaining a protected digital presence. (Hogan 2010).

7- The information obtained through stealing the identity is utilized in a lot of ways such like:

- Phishing, smishing, and vishing schemes that compromise your personal information: Phishing incidents transpire when cybercriminals impersonate representatives of renowned corporations or governmental bodies, deceiving individuals into divulging personal details, transferring funds, or installing malware on their devices. These attacks can manifest through emails, deceptive text messages (referred to as "smishing"), messages on social media

platforms, or telephone calls (referred to as "vishing").

- Lost or pilfered wallets: If someone steals your wallet (or purse), fraudulent individuals can potentially access your credit cards and identification. Even the mere possession of your driver's license can furnish enough personal information for a criminal to perpetrate identity fraud.

- Data breaches that expose passwords and confidential information: Identity theft is frequently triggered by data breaches, where unauthorized individuals infiltrate the services, you use and pilfer stored information. This may encompass your name, email address, passwords, credit card details, and even your Social Security number (SSN).

- Cyber intruders clandestinely monitoring public Wi-Fi: Public Wi-Fi networks found in places like coffee shops, airports, and hotels are known for their susceptibility to hacking. If hackers successfully breach the network to which you are connected, they can intercept and access all the data you transmit, including emails, passwords, and account numbers.

- Unscrupulous individuals purchasing your data on the Dark Web: The Dark Web constitutes an extensive network of websites and forums that remain inaccessible through standard web browsers, offering users an additional layer of anonymity. Within this hidden realm, cybercriminals engage in buying and selling information pilfered during data breaches.

- Malware attacks encompassing ransomware, spyware, and various viruses: Malware constitutes a form of cyber assault wherein hackers introduce malicious software into your devices. This software is capable of espionage, personal information theft, or locking your devices until a ransom is paid to the hacker.

- Synthetic identity theft: Synthetic identity theft occurs when criminals fabricate a "novel" identity by merging your Social Security Number (SSN) and other purloined data with either someone else's or entirely fictitious information. This composite identity, resembling a "Frankenstein" creation, is then utilized to initiate new bank accounts, acquire credit, or perpetrate other fraudulent activities — all under your name or SSN.

- Malevolent websites pilfering your login credentials: Not all websites guarantee security. Scammers frequently craft counterfeit websites resembling familiar ones, like your bank or Netflix login page. If you input your login details on these deceptive sites, the information goes directly to the fraudster. Some malicious websites are also engineered to contaminate your device with malware. Particularly hazardous sites can evade your device's built-in security, installing viruses that scour your computer for passwords and financial data.

- Observation of your sensitive information in public, known as "shoulder surfing": In instances of shoulder surfing, criminals clandestinely observe your digital device usage in public, aiming to pilfer your personal information. Typically, perpetrators maintain a safe distance to avoid detection. Nonetheless, they can discern finger movements as you type on a keypad. Additionally, they may employ binoculars, miniature cameras, or concealed cameras to surreptitiously monitor and eavesdrop on you. (aura) (Copes and Vieraitis, 2009a, 2009b, 2012; Duffin et al., 2006).

8- Identity Theft Consequences

8-1- The financial consequences (Randa & Reyns in 2019)

- Direct costs pertain to the financial gains obtained by an offender through the improper use of a victim's information.

- Indirect financial losses encompass expenses related to identity theft that do not benefit the perpetrator, such as costs associated with legal representation for victims. Fortunately, many victims of identity theft are reimbursed by their bank or credit card company, mitigating significant personal financial losses (Randa & Reyns, 2019).

- Out-of-pocket costs, for which victims of identity theft shared some responsibility for the fraudulent activities perpetrated against them, amounted to a total cost of 1.7 billion dollars in 2018, as reported by Marchini & Pascual in 2019.

- Potential harms could involve activities such as transaction fraud, theft of telecommunication services, electronic funds transfer crimes, electronic money laundering, and similar offenses.

8-2- Psychological and Emotional consequences

- Communal Anxiety: When community members fall victim to this digital theft, others may experience sensitive insecurity & anxiety, observing themselves as susceptible as well.

- Loss of Social Capital: The emotional peal of virtual identity theft can reduce user ability to actively participate in community activities, impacting social capital.

- Reputation Injury: Disseminating false information can inflict harm on a user's reputation within the community, potentially resulting in isolation.

- Breach of Trust and Violation of Privacy: Virtual identity theft entails a significant breach of trust and a violation of one's privacy. The emotional impact stems from the realization that personal data, has been ta without agreement.

- Sense of Powerlessness: Users of virtual identity theft often experience a sensitive sense of vulnerability. The realization that their personal data is no longer under Their dominance can lead to feelings of insecurity.

- Invasion of Personal Space: This type of theft of involves a significant attack of personal space. This intrusion into user's digital life can induce feelings of being invaded, leading to a sense of insecurity.

- Anxiety: Concerns about possible consequences is a common emotional feeling to virtual identity theft. Victims may fear the misappropriation of their stolen data, leading to financial loss, reputation damage, or legal implications.

- Loss of Control and Autonomy: This loss can result in sensitive stress as victims wrestle with the uncertainty of how their data will be used.

- Impact on Relationships: It can strain personal and professional relationships, potentially leading to a breakdown in trust.

- Long-Term Emotional Trauma: The emotional impact can extend into the long term. Even after resolving instant issues, users may last to experience lingering feelings of insecurity related to the defilement of their virtual identity.

-Difficulty Regaining a Sense of Security: Rebuilding the security after virtual identity theft can be hard. The fear of a recurrence may remain, making it hard for users to fully trust online space and engage in digital lives without anxiety. (Yar, M., & Steinmetz, K. F. 2019)

8-3- Less commonly, an identity thief may interfere with law enforcement by providing another person‘s identity upon arrest or during a criminal investigation or pull-over (Identity Theft Resource Center, 2003; Jasper, 2002), which is classified as secondary identity theft victimization by McQuade (2006). Under some extreme circumstances, victims of identity theft may suffer from being suspects of serious violence (e.g., murder) committed by identity thieves who un/intentionally leave the identifying means at the crime scene.

9- The basic preventative measures that one can take to decrease these risks

From a structural perspective, incorporating protective software into a computer system can diminish the risk of identity theft. Protective software encompasses anti-virus tools, ad-aware programs, and spyware detectors designed to identify and eliminate malicious software as well as sensitive personal information from individual computer systems (Bossler and Holt 2010; Choi 2008; Mell et al. 2005; Taylor et al. 2010). These programs are specifically crafted to lower the probability of malware infiltrating computer systems by scanning various files within the software (Bossler and Holt 2010; Choi 2008; Taylor et al. 2010).

Furthermore, the implementation of firewalls in a system can serve as a valuable protective measure against identity theft. Firewall programs exist in two variants: hardware and software (Szor 2005). Hardware firewalls are typically integrated into router technology and email servers to defend computer systems connected to a network. These technologies minimize the risk of attackers breaching network defenses to compromise individual computers (Nazario 2003; Szor 2005: Holt & Turner 2012).

10- The most important findings with respect to victims of such crimes concern the time taken to discover the crime:

- The longer it takes to discover the theft, the greater the victim’s loss and suffering.

- Low-income, less-educated victims take longer to discover or report

the crime, resulting in greater suffering, especially from harassment by debt collectors, utility cut-offs, and banking problems. (Chawki & Abdel Wahab 2006).

11- Prevalent Sensitive Personal Information Requisite for Identity Theft

- Social Security Numbers (SSN) — These number was created to keep an accurate record of earnings and pay retirement benefits on those earnings.

- Date of Birth (DOB) — Date of birth, in conjunction with other pieces of information, can be used in many ways to compromise a person's identity.

- Current and Previous Addresses and Phone Numbers — Both can be used in cybercrime and identity theft to enable an offender to assume the identity of the victim or to obtain more information thereabout.

- Current and Previous Employment Information — Such information can be used to jeopardize the victim's identity.

- Financial Account Information — This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is a rich source for an identity thief to commit financial cybercrimes.

- Mother's Maiden Name — In many instances, the maiden's name of the victim's mother may be used as the password for financial accounts and is easily available through public record information.

- Other Personal Information — This includes passwords, passcodes,

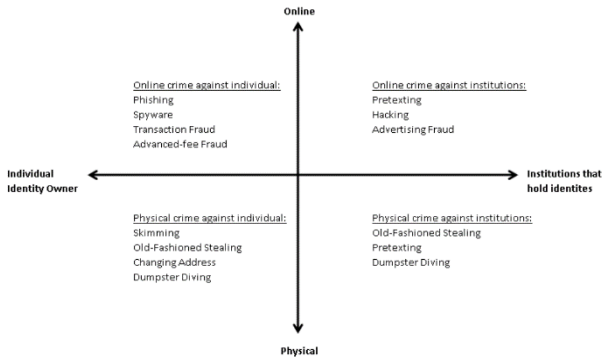
- email addresses as well as photos. Such information could be utilized to obtain access to other sensitive information or to facilitate total or partial identity theft. (Chawki and Abdel Wahab (2006).

12- The Elements and Methods Involved in Identity Theft

Acquiring others' identifying information is a task identity thieves accomplish through various means. The examples of identity theft are potentially only restricted by an individual's creativity but are consistently expanding due to technological advancements. In order to unravel the seemingly complex incidents of identity theft, we can utilize two dimensions. (Wang and Huang 2011)

The horizontal dimension focuses on the source from which identity thieves obtain the identifying information. At one end of this dimension is the individual victim, while at the other end are institutions that lawfully store clients' personal information. Generally, stealing an individual's personal information is easier compared to breaching the security protocols of institutions. However, when identity thieves successfully infiltrate the layers of protection employed by these institutions, the loss of identity information is often extensive, leading to more substantial damages. (Wang and Huang 2011)

The vertical dimension pertains to the location where the identity theft occurs. Identity thieves may either violate social rules in the physical world (such as stealing an individual victim's mail containing personal information or coercing institutions' employees with access to clients' personal information) or deceive users of various online services. At times, the financial repercussions of identity theft only commence when fraudsters purchase illegitimately collected identity information. Underground data warehouses that sell such information online can significantly contribute to financial disasters for individuals (Symantec, 2007). (Wang and Huang 2011)



13- Experimental

An experiment was conducted to test hypotheses by creating three short video advertisements aimed at raising awareness of virtual identity security. The study utilized a questionnaire adapted from Krugera

and Kearney (2006), administered both before and after the presentation of these short video ads on YouTube to assess their impact on Egyptian youth. The initial sample included 120 participants randomly selected from the YouTube platform (aged 20 to 40 years). However, 24 respondents were excluded due to incomplete responses, resulting in a final sample of 96 participants, comprising 60% men and 40% women. The three advertisements were displayed on the YouTube digital platform for broadcast to the research sample from June 2023 to January 2024.

13-1- Stimuli

Short video advertisements on visual identity security were featured on YouTube. The first ad had a duration of 1 minute and 34 seconds, the second ad lasted 1 minute and 30 seconds, and the third ad also lasted 1 minute. All three were created to investigate awareness regarding the importance of securing virtual identities. To ensure the suitability of the ad options for this research, a pre-test was conducted. Ten specialists were asked to watch the ads, and five minutes later, they were tested to recall the purpose.

13-2- Tools of the Study

The researcher utilized the Statistical Package for the Social Sciences (SPSS 25) to conduct statistical analyses and employed the following statistical methods:

- Pearson correlation coefficient.
- Cronbach's alpha coefficient.
- Frequency and percentage (relative weight).
- Mean and standard deviation.
- One Way Repeated-measured ANOVA.
- Bonferroni test for multiple comparisons.
- Eta squared (ηp2) equation for effect size calculation.

13-3- Measures

This survey questionnaire, designed to measure awareness levels on virtual identity security among youth, adapted from [Krugera & Kearney 2006] for the purpose of investigating the understanding, knowledge, and consciousness of young individuals regarding the safeguarding of their virtual identities in the digital landscape. The items cover various aspects, including the comprehension of virtual identity security, awareness of potential risks, recognition of cybercriminal tactics, understanding the importance of secure passwords, knowledge of privacy settings, awareness of consequences of online identity theft, ability to identify phishing attempts, consciousness of multi-factor authentication, familiarity with vulnerabilities associated with virtual identity, and knowledge of steps to take in case of virtual identity compromise. The questionnaire aims to contribute valuable insights to the field of awareness of virtual identity security of the youth in the digital age.

13-4- First Ad:

- The ad idea: The advertisement aims to highlight the risk of sharing personal identity information online. It humorously portrays everyday situations where the protagonist, a young man representing the target audience, realizes that his personal details are widely known and impacting him significantly.

- The ad Slogan: The internet possesses extensive knowledge about you, your virtual identity is in jeopardy.

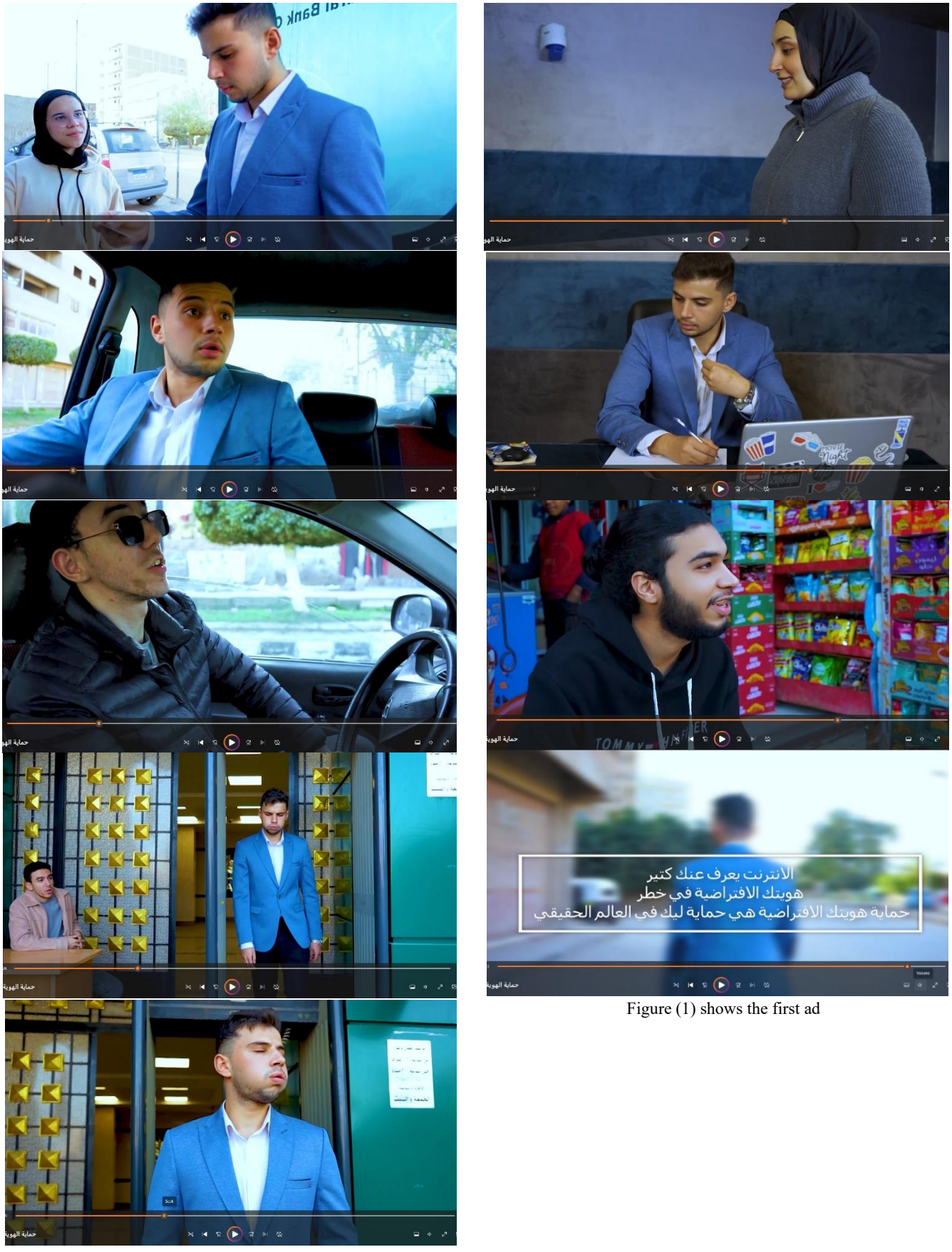
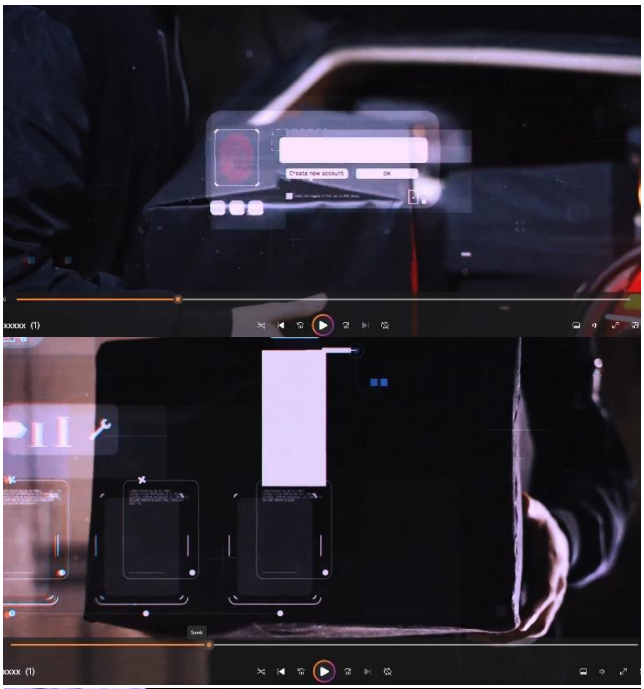


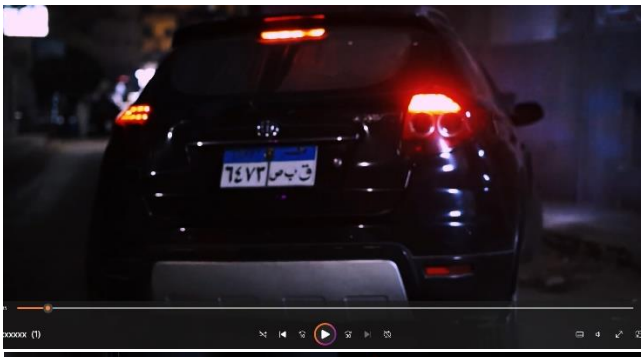
Figure (1) shows the first ad

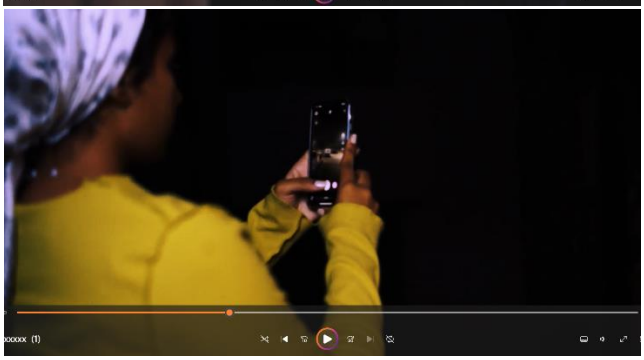
13-5- Second Ad:

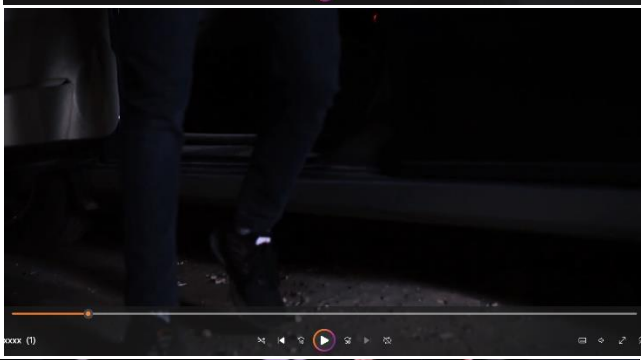
-The ad idea: The advertisement aims to illustrate how easily personal data can be stolen and virtual identities can be compromised in a symbolic manner, indicating the possibility of theft through various means. In the ad, a young man moves his cart to park beneath a girl's house, who herself becomes a victim of virtual identity theft. He then takes out a box from his cart and stands beneath the girl's house, where she opens her smartphone, unwittingly releasing her data through graphic shapes towards the box. The young man then drives away in his car, symbolizing the ease of virtual identity theft.

- The ad Slogan: Every piece of information you put online increases the opportunity for someone else to steal your virtual identity. If we don't take serious steps, we will all become victims of virtual identity theft.









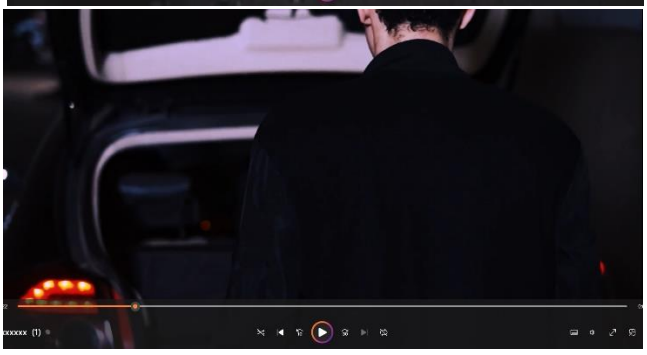
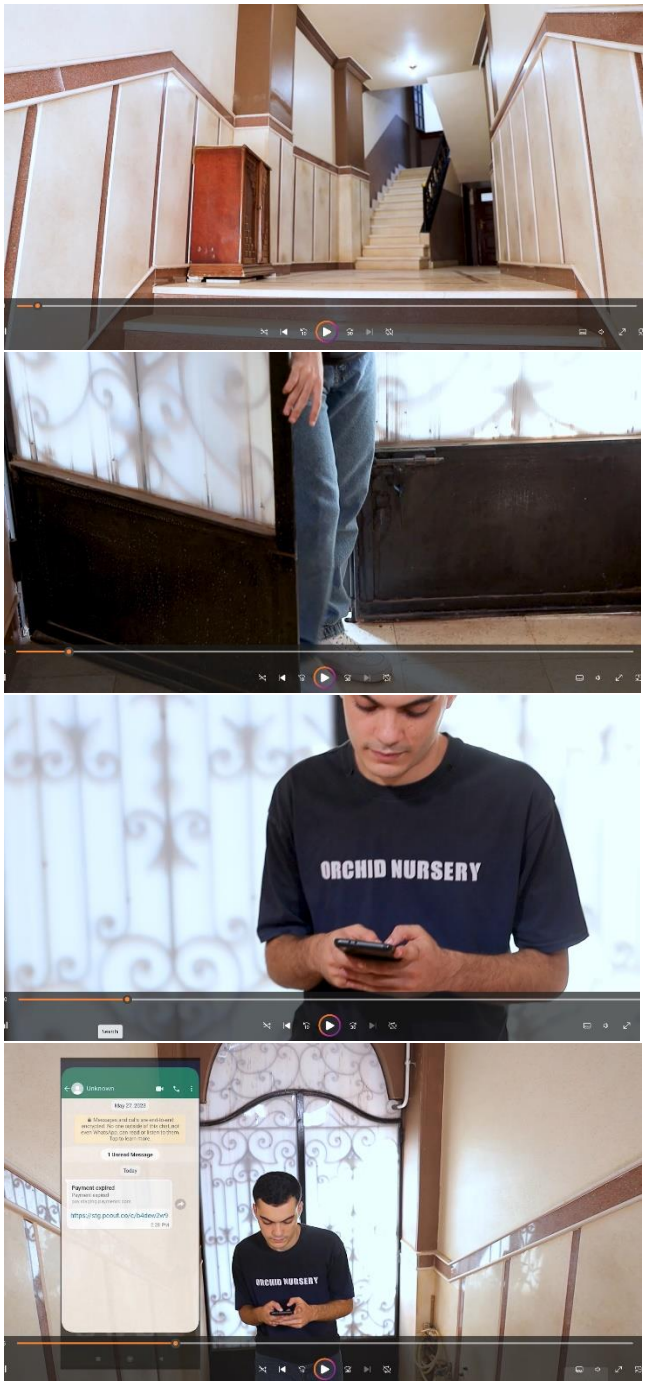


Figure (2) shows the second ad

13-6- Third Ad:

- The ad idea: The advertisement revolves around addressing the concept of the danger of virtual identity theft in a way that combines humorous strangeness, with the young man being the central character. He receives a link on one of the social media applications while returning home, only to discover a crowd of people moving his furniture outside his residence. This indicates the theft of his belongings, and the advertisement ends with him entering his empty house. In a comedic development, another young man appears carrying him, symbolizing how his life has become the property of those who stole his virtual identity.

-The ad Slogan: Your belongings, identity, or even your privacy could be stolen without you realizing it. Do not enter your personal data on any anonymous links.



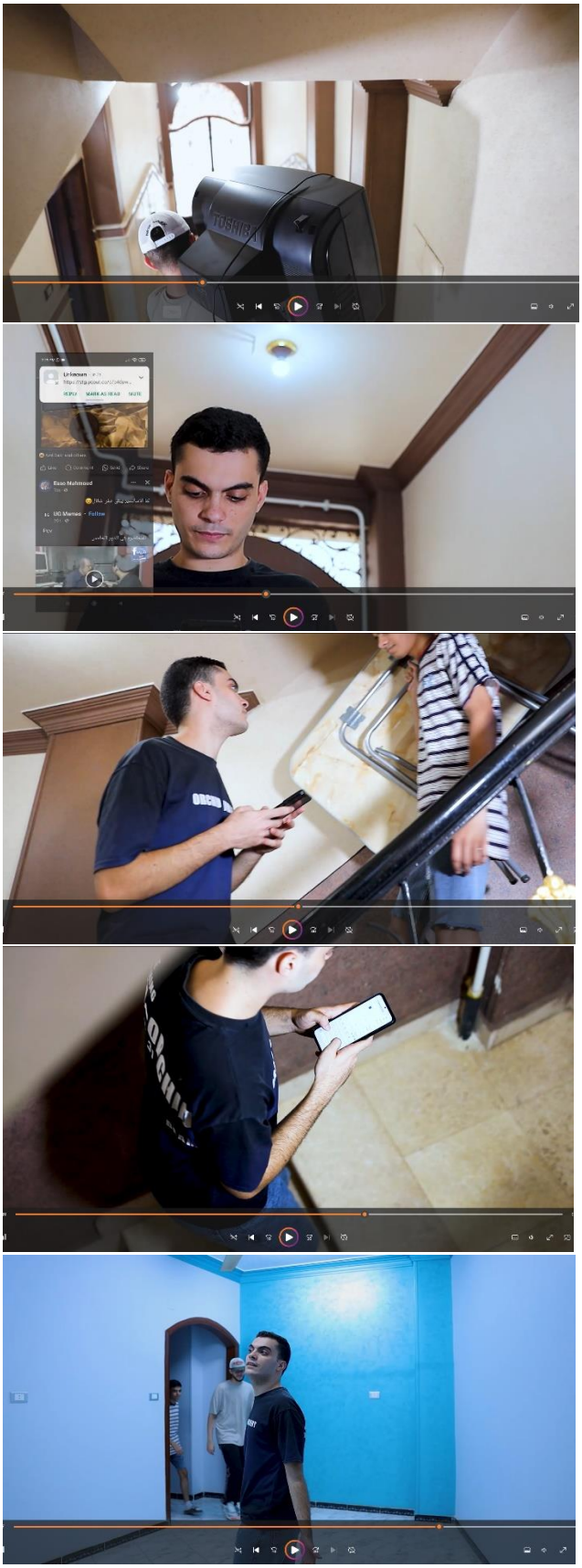


Figure (3) shows the third ad

14- Validity and Reliability of the Questionnaire Findings

14-1- Internal Consistency Validity Results

The results of internal consistency reliability were examined. To assess the internal consistency reliability of the questionnaire, the researcher calculated the correlation coefficient between the scores of each statement in the questionnaire and the total scores of the section to which the statement belongs. The results are presented in Table (1), showing the correlation coefficients between the scores of each statement in the questionnaire and the total scores of the section to which the statement belongs.

Questionnaire Sections	Item num	Correlation coefficient	Significance level	Statistical significance
First Section	١	٠,٧١	٠,٠١	Statistically significant
	٢	٠,٦٠	٠,٠١	Statistically significant
	٣	٠,٦٣	٠,٠١	Statistically significant
	٤	٠,٥٧	٠,٠١	Statistically significant
	٥	٠,٧١	٠,٠١	Statistically significant
	٦	٠,٦٥	٠,٠١	Statistically significant
	٧	٠,٥٤	٠,٠١	Statistically significant
	٨	٠,٥٥	٠,٠١	Statistically significant
	٩	٠,٦٠	٠,٠١	Statistically significant
	١٠	٠,٥١	٠,٠١	Statistically significant
Second Section	١١	٠,٥٤	٠,٠١	Statistically significant
	١٢	٠,٥٦	٠,٠١	Statistically significant
	١٣	٠,٥٥	٠,٠١	Statistically significant
	١٤	٠,٧١	٠,٠١	Statistically significant
	١٥	٠,٦٠	٠,٠١	Statistically significant
	١٦	٠,٦٤	٠,٠١	Statistically significant
	١٧	٠,٥٨	٠,٠١	Statistically significant

	١٨	٠,٥٦	٠,٠١	Statistically significant
	١٩	٠,٥١	٠,٠١	Statistically significant
	٢٠	٠,٧٣	٠,٠١	Statistically significant

Table (1) shows the correlation coefficients between the scores of each statement in the questionnaire and the total scores of the section to which the statement belongs. These coefficients ranged from 0.50 to 0.73, and all of them were statistically significant. Therefore, the questionnaire statements are considered reliable for the intended measurement.

15- Results of the construct validity of the questionnaire

To verify the construct validity of the questionnaire, the researcher calculated the correlation coefficient between the total scores of each section of the questionnaire and the total score of the questionnaire. The results are presented in Table.(٢)

Questionnaire sections	correlation coefficient	Significance level	Statistical significance
First Section	٠,٨٦	٠,٠١	**significance**
Second Section	٠,٨١	٠,٠١	**significance**

Table (2) illustrates the correlation coefficients between the scores of each section of the questionnaire and the total score of the questionnaire, which were (0.86, 0.81) respectively. These correlations were statistically significant, indicating the validity and homogeneity of the questionnaire sections.

15-1- Results of the questionnaire's reliability and its sections

To verify the reliability of the questionnaire and its sections, the researcher used Cronbach's alpha coefficient method. The results are presented in Table (3).

Questionnaire Sections	Items Num	Cronbach's alpha coefficient
First Section	١٠	٠,٨١
Second Section	١٠	٠,٧٩
Over All	٢٠	٠,٨٤

Table (3) displays the reliability coefficients for the questionnaire and its sections, which were (0.81, 0.79) for the questionnaire sections, and the reliability coefficient for the entire questionnaire was (0.96). These reliability coefficients are considered acceptable, providing the researcher with confidence in the results of the questionnaire application.

16- Results

16-1- Analysis of Field Study Results

In this study, the opinions of the research sample are presented and analyzed through a questionnaire regarding "Assessing the Effectiveness of Short Video Advertisements in Promoting Awareness of Virtual Identity Security among Youth." The aim of the research is to evaluate the effectiveness of short video advertisements in enhancing awareness among youth regarding the importance of virtual identity security and promoting safe online behavior for their virtual identities.

The responses of the research sample were assessed according to a five-point Likert scale as follows:

The opinion	agreement				
	Strongly agree	Strongly agree	Neutral	disagree	Disagree Strongly
weight	٥	٤	٣	٢	١
Weighted average	٥ – ٤,٢٠	٣,٤٠ – ٤,١٩	٢,٦٠ – ٣,٣٩	١,٨٠ – ٢,٥٩	١,٧٩ –١

Table (1): Five-point Likert Scale

Note: All means, standard deviations, and relative weights are rounded to the nearest two decimal places.

16-2- Results of the statistical analysis for the questionnaire before exposure to short video advertisements:

Ranking	Degree of approval	Relative weight (%)	standard deviation	SMA	Total weights	ITems	items
٥	Strongly Disagree	٪٣٥,٢٠	٠,٧٦	١,٧٦	١٦٩	I agree that I have a clear understanding of what virtual identity security entails.	١
١	not agree	٪٣٨,٤٠	٠,٨٥	١,٩٢	١٨٤	I agree that I am aware of the potential risks associated with sharing personal information online.	٢
٧	Strongly Disagree	٪٣٣,٢٠	٠,٦٣	١,٦٦	١٥٩	I agree that I can identify common methods used by cybercriminals to compromise virtual identities.	٣
٣	not agree	٪٣٦,٦٠	٠,٧٥	١,٨٣	١٧٦	I agree that I understand the importance of using secure passwords for my online accounts.	٤
٤	not agree	٪٣٦,٤٠	٠,٧٨	١,٨٢	١٧٥	I agree that I recognize the importance of regularly updating my privacy settings on social media platforms.	٥
٦	Strongly	٪٣٤,٢٠	٠,٧٢	١,٧١	١٦٤	I agree that I am	٦

	Disagree					aware of the potential consequences of falling victim to online identity theft.	
٢	not agree	٪٣٧,٨٠	٠,٧٨	١,٨٩	١٨١	I agree that I have knowledge of how to recognize and avoid phishing attempts targeting virtual identities.	٧
٩	Strongly Disagree	٪٣١,٨٠	٠,٧٣	١,٥٩	١٥٣	I agree that I understand the importance of multi-factor authentication to enhance virtual identity security.	٨
٨	Strongly Disagree	٪٣٢,٢٠	٠,٦٩	١,٦١	١٥٥	I agree that I am well-informed about the vulnerabilities associated with virtual identities in online environments.	٩
١٠	Strongly Disagree	٪٣١,٤٠	٠,٦٩	١,٥٧	١٥١	I agree that I am aware of the steps to take in case my virtual identity is compromised.	١٠
Strongly Disagree		٪٣٤,٨٠	٠,٣٧	١,٧٤	Overall assessment of the first section before exposure to short video advertisements		
١٠	Strongly Disagree	٪٣٢,٦٠	٠,٧٤	١,٦٣	١٥٦	I agree that I have made changes to my password practices (for example, using stronger passwords and changing them regularly) after becoming aware of virtual identity security.	١١
٩	Strongly Disagree	٪٣٢,٨٠	٠,٦٢	١,٦٤	١٥٧	I agree that I have become more cautious about sharing personal information online due to awareness of virtual identity security risks.	١٢
٤	not agree	٪٣٦,٦٠	٠,٨٠	١,٨٣	١٧٦	I agree that I now actively review and update privacy settings on my social media accounts.	١٣
٣	not agree	٪٣٧,٢٠	٠,٧٢	١,٨٦	١٧٩	I agree that I have started using two-factor authentication for my online accounts as a result of increased awareness of virtual identity security.	١٤
٧	Strongly Disagree	٪٣٤,٠٠	٠,٦٧	١,٧٠	١٦٣	I agree that I am more vigilant in recognizing and avoiding	١٥
						potential phishing attempts.	
٨	Strongly Disagree	٪٣٣,٦٠	٠,٥٧	١,٦٨	١٦١	I agree that I have reduced the amount of personal information shared on public platforms or websites.	١٦
٦	Strongly Disagree	٪٣٥,٤٠	٠,٦٧	١,٧٧	١٧٠	I agree that I now regularly monitor my online accounts for any unusual or unauthorized activity.	١٧
٥	not agree	٪٣٦,٤٠	٠,٧٧	١,٨٢	١٧٥	I agree that I am more cautious about the websites and applications I use to ensure they are secure.	١٨
١	not agree	٪٣٨,٢٠	٠,٧٤	١,٩١	١٨٣	I agree that I have changed my online behavior to minimize the use of public Wi-Fi networks for sensitive activities.	١٩
٢	not agree	٪٣٧,٨٠	٠,٦٩	١,٨٩	١٨١	I agree that I have become more proactive in educating friends and family about virtual identity security practices.	٢٠
Strongly Disagree		٪٣٥,٤٠	٠,٣٤	١,٧٧	Overall assessment of the second section before exposure to short video advertisements		
Strongly Disagree		٪٣٥,٠٠	٠,٣١	١,٧٥	Overall assessment of the questionnaire before exposure to short video advertisements		

Table (2): Means, standard deviations, relative weights, and agreement level of responses from the research sample towards the questionnaire statements before exposure to short video advertisements.

Table (2) illustrates the levels of responses from the research sample regarding youth awareness levels concerning the importance of virtual identity security and the level of safe online behavior for their virtual identities before exposure to short video advertisements. Responses to the questionnaire statements ranged from "Strongly Disagree" to "Disagree". The results are as follows:

Level 1: Awareness levels for the questionnaire assessing awareness of virtual identity security among youth before exposure to short video advertisements.

Responses fell into the "Disagree" level for statements numbered (2, 4, 5, 7), with the arithmetic mean values ranging between (1.82 – 1.92), and relative weights ranging between (36.40% – 38.40%).

Responses fell into the "Strongly Disagree" level for the remaining statements of the first section, with arithmetic mean values ranging between (1.51 – 1.76), and relative weights ranging between (31.40% – 35.20%). The arithmetic mean for the first section before exposure to short video advertisements was (1.74) with a relative weight of (34.80%), indicating a "Strongly Disagree" degree.

Level 2: Assessment of self-reported behavioral changes regarding virtual identity security among youth before exposure to short video advertisements.

Responses fell into the "Disagree" level for statements numbered (13, 14, 18, 19, 20), with arithmetic mean values ranging between (1.82 – 1.91), and relative weights ranging between (36.40% – 38.20%). Responses fell into the "Strongly Disagree" level for the remaining statements of the second section, with arithmetic mean values ranging between (1.63 – 1.77), and relative weights ranging between (32.60% – 35.40%). The arithmetic mean for the second section before exposure to short video advertisements was (1.77) with a relative weight of (35.40%), indicating a "Strongly Disagree" degree.

The overall arithmetic mean for the entire questionnaire before exposure to short video advertisements was (1.75) with a relative weight of (35.0%), indicating a "Strongly Disagree" degree.

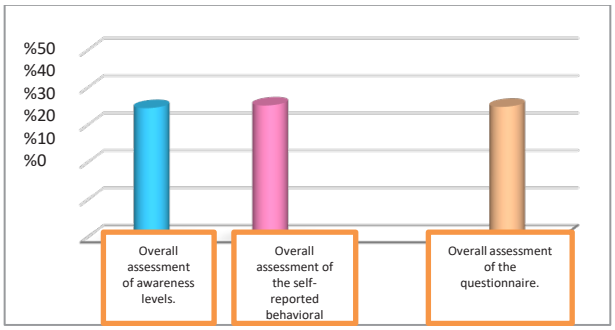


Figure (4): Illustrates the relative weights for the overall assessment of the first section, the second section, and the entire questionnaire before exposure to short video advertisements.

Ranking	Degree of approval	Relative weight (%)	standard deviation	SMA	Total weights	ITems	items
٣	agree	٦٩,٠٠٪	٠,٦٥	٣,٤٥	٣٣١	I agree that I have a clear understanding of what virtual identity security entails.	١
٦	NA	٦٤,٨٠٪	٠,٨٠	٣,٢٤	٣١١	I agree that I am aware of the potential risks associated with sharing personal information online.	٢
٨	NA	٦٣,٨٠٪	٠,٧٢	٣,١٩	٣٠٦	I agree that I can identify common methods used by cybercriminals to compromise virtual identities.	٣
٧	NA	٦٤,٢٠٪	٠,٧٤	٣,٢١	٣٠٨	I agree that I understand the importance of using secure passwords for my online accounts.	٤
٤	agree	٦٨,٤٠٪	٠,٩٠	٣,٤٢	٣٢٨	I agree that I recognize the importance of regularly updating my privacy settings on social media platforms.	٥
٩	NA	٦٢,٦٠٪	٠,٩١	٣,١٣	٣٠٠	I agree that I am aware of the potential consequences of falling victim to online identity theft.	٦
٥	NA	٦٧,٠٠٪	٠,٨١	٣,٣٥	٣٢٢	I agree that I have knowledge of how to recognize and avoid phishing attempts targeting virtual identities.	٧
١٠	NA	٦٢,٦٠٪	١,٠٠	٣,١٣	٣٠٠	I agree that I understand the importance of multi-factor authentication to enhance virtual identity security.	٨
٢	agree	٦٩,٤٠٪	٠,٨٩	٣,٤٧	٣٣٣	I agree that I am well-informed about the vulnerabilities associated with virtual identities in online environments.	٩
١	agree	٧٢,٠٠٪	٠,٨٣	٣,٦٠	٣٤٦	I agree that I am aware of the steps to take in case my virtual identity is compromised.	١٠
NA		٦٦,٤٠٪	٠,٤٩	٣,٣٢	Overall assessment of the first section before exposure to short video advertisements		
٣	agree	٦٨,٦٠٪	٠,٨٤	٣,٤٣	٣٢٩	I agree that I have made changes to my password practices (for example, using stronger passwords and changing them regularly) after becoming aware of virtual identity security.	١١
٢	agree	٧٠,٨٠٪	٠,٩٣	٣,٥٤	٣٤٠	I agree that I have become more cautious about sharing personal	١٢

						information online due to awareness of virtual identity security risks.	
٥	NA	٪٦٧,٢٠	٠,٩٣	٣,٣٦	٣٢٣	I agree that I now actively review and update privacy settings on my social media accounts.	١٣
٩	NA	٪٦٥,٢٠	١,٠٥	٣,٢٦	٣١٣	I agree that I have started using two-factor authentication for my online accounts as a result of increased awareness of virtual identity security.	١٤
٤	agree	٪٦٨,٦٠	٠,٨٧	٣,٤٣	٣٢٩	I agree that I am more vigilant in recognizing and avoiding potential phishing attempts.	١٥
١	agree	٪٧٤,٢٠	١,٠٣	٣,٧١	٣٥٦	I agree that I have reduced the amount of personal information shared on public platforms or websites.	١٦
٦	NA	٪٦٧,٠٠	٠,٩٢	٣,٣٥	٣٢٢	I agree that I now regularly monitor my online accounts for any unusual or unauthorized activity.	١٧
٧	NA	٪٦٥,٦٠	٠,٩٧	٣,٢٨	٣١٥	I agree that I am more cautious about the websites and applications I use to ensure they are secure.	١٨
١٠	NA	٪٦٤,٤٠	٠,٩٢	٣,٢٢	٣٠٩	I agree that I have changed my online behavior to minimize the use of public Wi-Fi networks for sensitive activities.	١٩
٧	NA	٪٦٥,٢٠	١,٠٠	٣,٢٦	٣١٣	I agree that I have become more proactive in educating friends and family about virtual identity security practices.	٢٠
NA		٪٦٧,٦٠	٠,٦٨	٣,٣٨	Overall assessment of the second section before exposure to short video advertisements		
NA		٪٦٧,٠٠	٠,٥٢	٣,٣٥	Overall assessment of the questionnaire before exposure to short video advertisements		

Table (3) below illustrates the response levels of the research sample regarding the levels of awareness among young people regarding the importance of virtual identity security and the level of safe behavior and practices online for their virtual identities after exposure to the first advertisement. Responses were categorized as (Agree, Neutral), The results were as follows:

Level 1: Awareness levels for the questionnaire assessing awareness of virtual identity security among youth after the first advertisement.

Responses fell into the "Agree" level for statements numbered (1, 5, 9, 10), with arithmetic mean values ranging between (3.42 – 3.60), and relative weights ranging between (68.40% – 72.0%). Responses fell into the "Neutral" level for the remaining statements of the first section, with arithmetic mean values ranging between (3.13 – 3.35), and relative weights ranging between (62.60% – 67.0%). The arithmetic mean for the first section after the first advertisement was (3.32) with a relative weight of (66.40%), indicating a "Neutral" degree.

Level 2: Assessment of self-reported behavioral changes regarding virtual identity security among youth after the first advertisement.

Responses fell into the "Agree" level for statements numbered (11, 12, 15, 16), with arithmetic mean values ranging between (3.43 – 3.71), and relative weights ranging between (68.60% – 74.20%). Responses fell into the "Neutral" level for the remaining statements of the second section, with arithmetic mean values ranging between (3.22 – 3.36), and relative weights ranging between (64.40% – 67.20%). The arithmetic mean for the second section after the first advertisement was (3.38) with a relative weight of (67.60%) and a "Neutral" degree.

The overall arithmetic mean for the entire questionnaire after the first advertisement was (3.35) with a relative weight of (67.0%) and a "Neutral" degree.

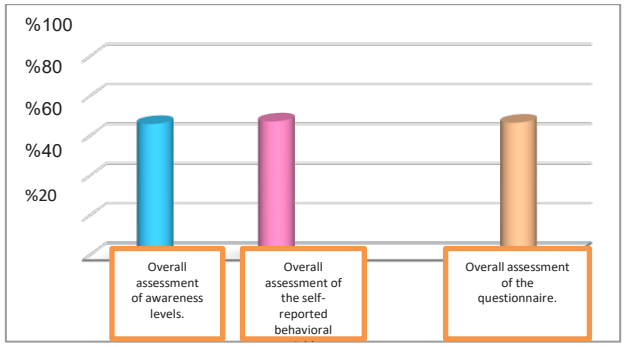


Figure (5): Illustrates the relative weights for the overall assessment of the first section, the second section, and the entire questionnaire after the first advertisement.

16-3- Statistical results for the questionnaire after the second advertisement:

Table (4): Arithmetic means, standard deviations, relative weights, and agreement level of responses from the research sample towards the questionnaire statements after the second advertisement.

Ranking	Degree of approval	Relative weight (%)	standard deviation	SMA	Total weights	ITems	items
٢	Strongly agree	٪٨٥,٨٠	٠,٩٤	٤,٢٩	٤١٢	I agree that I have a clear understanding of what virtual identity security entails.	١
١٠	agree	٪٧٣,٢٠	٠,٨٦	٣,٦٦	٣٥١	I agree that I am aware of the potential risks associated with sharing personal information online.	٢
٨	agree	٪٧٦,٢٠	٠,٨٥	٣,٨١	٣٦٦	I agree that I can identify common methods used by cybercriminals to compromise virtual identities.	٣
٥	agree	٪٧٧,٦٠	٠,٨٦	٣,٨٨	٣٧٢	I agree that I understand the importance of using secure passwords for my online accounts.	٤
٦	agree	٪٧٧,٠٠	٠,٨٩	٣,٨٥	٣٧٠	I agree that I recognize the importance of regularly updating my privacy settings on social media platforms.	٥
١	Strongly agree	٪٨٦,٦٠	٠,٩٠	٤,٣٣	٤١٦	I agree that I am aware of the potential consequences of falling victim to online identity theft.	٦
٩	agree	٪٧٣,٨٠	٠,٩٣	٣,٦٩	٣٥٤	I agree that I have knowledge of how to recognize and avoid phishing attempts targeting virtual identities.	٧
٣	Strongly agree	٪٨٤,٤٠	٠,٩٤	٤,٢٢	٤٠٥	I agree that I understand the importance of multi-factor authentication to enhance virtual identity security.	٨
٧	agree	٪٧٦,٦٠	٠,٩٥	٣,٨٣	٣٦٨	I agree that I am well-informed about the vulnerabilities associated with virtual identities in online environments.	٩
٤	Strongly agree	٪٨٤,٢٠	٠,٩٦	٤,٢١	٤٠٤	I agree that I am aware of the steps to take in case my virtual identity is compromised.	١٠
agree		٪٧٩,٦٠	٠,٥٠	٣,٩٨	Overall assessment of the first section before exposure to short video advertisements		
١	Strongly agree	٪٨٦,٨٠	٠,٩٥	٤,٣٤	٤١٧	I agree that I have made changes to my password practices (for example, using stronger passwords and changing them regularly) after becoming aware of virtual identity security.	١١
٤	agree	٪٨١,٦٠	١,٠٠	٤,٠٨	٣٩٢	I agree that I have become more cautious about sharing personal information online due to awareness of virtual identity security risks.	١٢
٧	agree	٪٦٩,٨٠	٠,٨٧	٣,٤٩	٣٣٥	I agree that I now actively review and update privacy settings on my social media accounts.	١٣
٦	agree	٪٧٧,٢٠	٠,٩٦	٣,٨٦	٣٧١	I agree that I have started using two-factor authentication for my online accounts as a result of increased awareness of virtual identity security.	١٤
٥	agree	٪٨١,٢٠	٠,٩٤	٤,٠٦	٣٩٠	I agree that I am more vigilant in recognizing and avoiding potential phishing attempts.	١٥
٢	Strongly agree	٪٨٤,٤٠	٠,٩٨	٤,٢٢	٤٠٥	I agree that I have reduced the amount of personal information shared on public platforms or websites.	١٦
١٠	agree	٪٦٨,٦٠	٠,٧٤	٣,٤٣	٣٢٩	I agree that I now regularly monitor my online accounts for any unusual or unauthorized activity.	١٧
٨	agree	٪٦٩,٤٠	٠,٧٩	٣,٤٧	٣٣٣	I agree that I am more cautious about the websites and applications I use to ensure they are secure.	١٨
٩	agree	٪٦٩,٢٠	٠,٧٩	٣,٤٦	٣٣٢	I agree that I have changed my online behavior to minimize the use	١٩

						of public Wi-Fi networks for sensitive activities.	
٣	agree	٪٨٣,٢٠	٠,٨٦	٤,١٦	٣٩٩	I agree that I have become more proactive in educating friends and family about virtual identity security practices.	٢٠
agree		٪٧٧,٢٠	٠,٥١	٣,٨٦	Overall assessment of the second section after the second advertisement.		
أوافق		٪٧٨,٤٠	٠,٤٤	٣,٩٢	Overall assessment of the questionnaire after the second advertisement.		

Table (4): Shows the levels of responses from the research sample towards levels of awareness among youth regarding the importance of virtual identity security and the level of safe behavior and practices online for their virtual identities after the second advertisement. Responses were categorized as (Strongly Agree, Agree), and the results are as follows:

Level 1: Awareness levels for the questionnaire assessing awareness of virtual identity security among youth after the second advertisement.

Responses fell into the "Strongly Agree" level for statements numbered (1, 6, 8, 10), with arithmetic mean values ranging between (4.21 – 4.33), and relative weights ranging between (84.20% – 86.60%). Responses fell into the "Agree" level for the remaining statements of the first section, with arithmetic mean values ranging between (3.43 – 3.88), and relative weights ranging between (73.20% – 77.60%). The arithmetic mean for the first section after the second advertisement was (3.98) with a relative weight of (77.20%) and an "Agree" degree.

Level 2: Assessment of self-reported behavioral changes regarding virtual identity security among youth after the second advertisement.

Responses fell into the "Strongly Agree" level for statements numbered (11, 16), with arithmetic mean values ranging between (4.34, 4.22) and relative weights (86.60%, 84.40%). Responses fell into the "Agree" level for the remaining statements of the second section, with arithmetic mean values ranging between (3.43 – 4.16) and relative weights ranging between (68.60% – 83.20%). The arithmetic mean for the second section after the second advertisement was (3.86) with a relative weight of (77.20%) and an "Agree" degree.

The overall arithmetic mean for the entire questionnaire after the second advertisement was (3.92) with a relative weight of (78.40%) and an "Agree" degree.

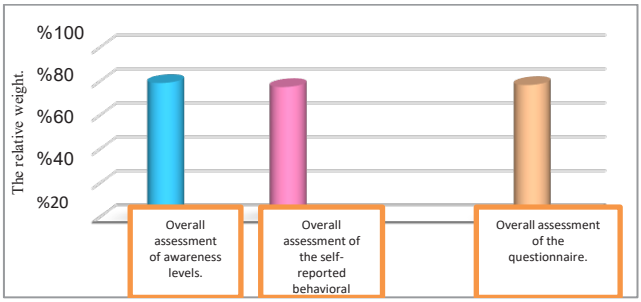


Figure (6): Illustrates the relative weights for the overall assessment of the first section, the second section, and the entire questionnaire after the third advertisement.

16-4- Statistical results for the questionnaire after the third advertisement:

Ranking	Degree of approval	Relative weight (%)	standard deviation	SMA	Total weights	ITems	items
١٠	Strongly agree	٪٨٩,٤٠	٠,٧٨	٤,٤٧	٤٢٩	I agree that I have a clear understanding of what virtual identity security entails.	١
٥	Strongly agree	٪٩٣,٦٠	٠,٤٧	٤,٦٨	٤٤٩	I agree that I am aware of the potential risks associated with sharing personal information online.	٢
٨	Strongly agree	٪٩٣,٢٠	٠,٤٨	٤,٦٦	٤٤٧	I agree that I can identify common methods used by cybercriminals to compromise virtual identities.	٣
٩	Strongly agree	٪٩٢,٦٠	٠,٤٩	٤,٦٣	٤٤٤	I agree that I understand the importance of using secure passwords for my online accounts.	٤
٤	Strongly agree	٪٩٣,٨٠	٠,٤٧	٤,٦٩	٤٥٠	I agree that I recognize the importance of regularly updating my privacy settings on social media platforms.	٥
٢	Strongly agree	٪٩٦,٤٠	٠,٣٨	٤,٨٢	٤٦٣	I agree that I am aware of the potential	٦

	social media accounts.						
١٤	I agree that I have started using two-factor authentication for my online accounts as a result of increased awareness of virtual identity security.	٤٥٥	٤,٧٤	٠,٤٤	٪٩٤,٨٠	Strongly agree	٥
١٥	I agree that I am more vigilant in recognizing and avoiding potential phishing attempts.	٤٥٦	٤,٧٥	٠,٤٤	٪٩٥,٠٠	Strongly agree	٤
١٦	I agree that I have reduced the amount of personal information shared on public platforms or websites.	٤٦٤	٤,٨٣	٠,٣٧	٪٩٦,٦٠	Strongly agree	٢
١٧	I agree that I now regularly monitor my online accounts for any unusual or unauthorized activity.	٤٤٦	٤,٦٥	٠,٤٨	٪٩٣,٠٠	Strongly agree	٨
١٨	I agree that I am more cautious about the websites and applications I use to ensure they are secure.	٤٤٤	٤,٦٣	٠,٤٩	٪٩٢,٦٠	Strongly agree	١٠
١٩	I agree that I have changed my online behavior to minimize the use of public Wi-Fi networks for sensitive activities.	٤٤٥	٤,٦٤	٠,٤٨	٪٩٢,٨٠	Strongly agree	٩
٢٠	I agree that I have become more proactive in educating friends and family about virtual identity security practices.	٤٥١	٤,٧٠	٠,٤٦	٪٩٤,٠٠	Strongly agree	٧
Overall assessment of the second section after the third advertisement.		٤,٧٣	٠,٢٥	٪٩٤,٦٠	**Strongly agree**		
Overall assessment of the questionnaire after the		٤,٧١	٠,٢٠	٪٩٤,٢٠	**Strongly agree**		

	consequences of falling victim to online identity theft.						
٧	I agree that I have knowledge of how to recognize and avoid phishing attempts targeting virtual identities.	٤٤٩	٤,٦٨	٠,٤٧	٪٩٣,٦٠	Strongly agree	٥ مكرر
٨	I agree that I understand the importance of multi-factor authentication to enhance virtual identity security.	٤٥٨	٤,٧٧	٠,٤٢	٪٩٥,٤٠	Strongly agree	٣
٩	I agree that I am well-informed about the vulnerabilities associated with virtual identities in online environments.	٤٤٨	٤,٦٧	٠,٤٧	٪٩٣,٤٠	Strongly agree	٧
١٠	I agree that I am aware of the steps to take in case my virtual identity is compromised.	٤٦٤	٤,٨٣	٠,٣٧	٪٩٦,٦٠	Strongly agree	١
Overall assessment of the first section before exposure to short video advertisements		٤,٦٩	٠,٢٣	٪٩٣,٨٠	**Strongly agree**		
١١	I agree that I have made changes to my password practices (for example, using stronger passwords and changing them regularly) after becoming aware of virtual identity security.	٤٦٦	٤,٨٥	٠,٣٥	٪٩٧,٠٠	Strongly agree	١
١٢	I agree that I have become more cautious about sharing personal information online due to awareness of virtual identity security risks.	٤٦٢	٤,٨١	٠,٣٩	٪٩٦,٢٠	Strongly agree	٣
١٣	I agree that I now actively review and update privacy settings on my	٤٥٤	٤,٧٣	٠,٤٥	٪٩٤,٦٠	Strongly agree	٦

				third advertisement.

Table (5): Arithmetic means, standard deviations, relative weights, and agreement level of responses from the research sample towards the questionnaire statements after the third advertisement.

Table (5) illustrates the levels of responses from the research sample regarding the awareness levels among young people regarding the importance of virtual identity security and the level of safe behavior and practices online for their virtual identities after the third advertisement. The responses to the questionnaire statements were in the level of "Strongly Agree," and the results are as follows:

Level 1: Awareness levels for the questionnaire assessing awareness of virtual identity security among young people after the third advertisement:

The responses were in the "Strongly Agree" level for all statements in the first section, with the average values ranging from (4.47 – 4.83), and the relative weights ranging from (89.40% – 96.60%). The average score for the first section after the third advertisement was (4.69) with a relative weight of (93.80%) and a "Strongly Agree" rating.

Level 2: Evaluation of self-reported behavioral changes regarding virtual identity security among young people after the third advertisement:

The responses were in the "Strongly Agree" level for all statements in the second section, with the average values ranging from (4.63 – 4.85), and the relative weights ranging from (92.60% – 97.0%). The average score for the second section after the third advertisement was (4.73) with a relative weight of (94.60%) and a "Strongly Agree" rating.

The overall average score for the questionnaire after the third advertisement was (4.71) with a relative weight of (94.20%) and a "Strongly Agree" rating.

Figure (4) illustrates the relative weights for the overall assessment of the first section, the second section, and the questionnaire as a whole after the third advertisement.

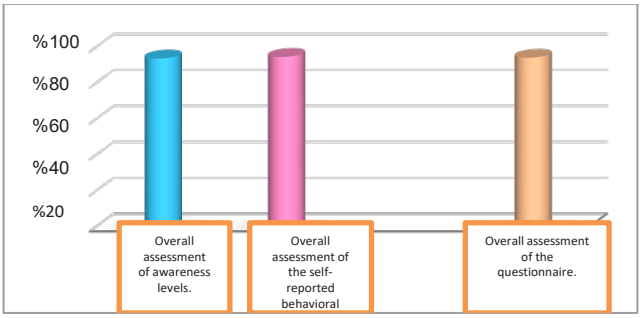


Figure (7) illustrates the relative weights for the overall assessment of the first section, the second section, and the questionnaire as a whole after the third advertisement.

17- Results of Statistical Hypothesis Testing for the Research:

17-1- First Hypothesis Results:

The first hypothesis states that "There are statistically significant differences at a significance level (≥ 0.05) between the mean scores of responses of the youth sample before and after exposure to short advertisements aimed at promoting awareness of virtual identity security among youth".

To verify this hypothesis, the researcher employed the One Way Repeated-measured ANOVA test, Bonferroni test for multiple comparisons, and the Eta squared (ηp2) equation to calculate the effect size for the short advertisements. Cohen's interpretation of the "effect size" value was utilized, where it is considered small if its value is (0.01), medium if its value is (0.06), and large if its value is (0.14). The results are as follows:

Source of variance	Sum of squares	Degrees of freedom	Mean squares	F	Significance level	Eta square
Groups (repeated measures)	٤٥٧,٣٤	٢,٠٦	٢٢١,٧٠	٨٢٦,٦٠	٠,٠٠١	٠,٨٩٧
The error	٥٢,٥٦	١٩٥,٩٧	٠,٢٧			

Table (1): Results of One Way Repeated-measured ANOVA for the Effect of Short Advertisements on Enhancing Awareness of Virtual Identity Security among Youth.

The table (1) indicates statistically significant differences between the mean scores of repeated measurements for levels of awareness of virtual identity security among youth before and after exposure to short advertisements, with an "F" value

of (826.60) and a significance level of (0.001). The Eta squared value (0.897) is greater than 0.14, as defined by Cohen for a large effect size. This suggests that the short advertisements shown to the research sample had a significant impact on enhancing awareness of virtual identity security among youth. Table (2) illustrates the results of the Bonferroni test for multiple comparisons to determine the directions and significance of differences between the mean scores of repeated measurements before and after exposure to short advertisements.

Groups (repeated measures)	SMA	Before showing the advertisements	After showing the first advertisement	After showing the second advertisement	After showing the third advertisement
Before showing the advertisements	١,٧٤	–	*١,٥٨١-	*٢,٢٤١-	*٢,٩٥٢-
After showing the first advertisement	٣,٣٢	–	–	*٠,٦٥٩-	*١,٣٧١-
After showing the second advertisement	٣,٩٨	–	–	–	*٠,٧١١-
After showing the third advertisement	٤,٦٩	–	–	–	–

Table (2): Illustrates the results of multiple comparisons between the mean scores of repeated measurements before and after exposure to short advertisements.
*Significant at the significance level of 0.05

From Table (2), it is evident that there are statistically significant differences between the mean scores of repeated measurements for the responses of the youth sample according to pairwise comparisons. Differences between the mean scores of repeated measurements before and after exposure to short advertisements are observed, indicating the significant impact of the advertisements in gradually enhancing awareness of virtual identity security among youth.

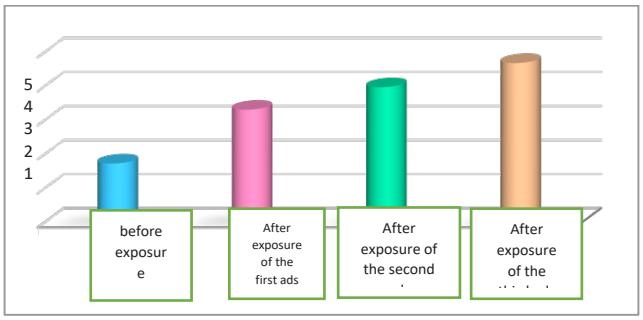


Figure (8): Illustrates the mean scores of measurements for levels of awareness of virtual identity security among youth gradually before and after exposure to short advertisements.

From Tables (1) and (2), along with their results, and Figure (8), it is evident that the first statistical hypothesis of the research has been achieved.

17-2- Results of the Second Statistical Hypothesis:

The second hypothesis states that "There are statistically significant differences at a significance level (≥ 0.05) between the mean scores of responses of the youth sample before and after exposure to short advertisements aimed at enhancing self-reported behavioral changes regarding virtual identity security among youth."

To verify this hypothesis, the researcher employed the One Way Repeated-measured ANOVA test, Bonferroni test for multiple comparisons, and the Eta squared (η_p^2) equation to calculate the effect size for the short advertisements. Cohen's interpretation of the "effect size" value was utilized, where it is considered small if its value is (0.01), medium if its value is (0.06), and large if its value is (0.14). The results are as follows:

Source of variance	Sum of squares	Degrees of freedom	Mean squares	F	Significance level	Eta square
Groups (repeated measures)	٤٤٤,٤٦	٢,٠٨	٢١٣,٢٨	٥٨٥,٧٥	٠,٠٠١	٠,٨٦٠
The error	٧٢,٠٩	١٩٧,٩٨	٠,٣٦			

Table (3): Results of One Way Repeated-measured ANOVA for the Effect of Short Advertisements on Enhancing Self-Reported

Behavioral Changes Regarding Virtual Identity Security among Youth.

It is evident from Table (3) that there are statistically significant differences between the mean scores of repeated measurements for self-reported behavioral changes regarding virtual identity security among youth before and after exposure to short advertisements. The "F" value is (585.75) with a significance level of (0.001). The Eta squared value is (0.860), which is greater than 0.14, as defined by Cohen for a large effect size. This indicates that the short advertisements shown to the research sample had a significant impact on enhancing awareness of virtual identity security among youth.

Groups (repeated measures)	SMA	Before showing the advertisements	After showing the first advertisement	After showing the second advertisement	After showing the third advertisement
Before showing the advertisements	١,٧٧	–	-*١,٦١٢	*٢,٠٨٥-	*٢,٩٦٠-
After showing the first advertisement	٣,٣٨	–	-	*٠,٤٧٣-	*١,٣٤٨-
After showing the second advertisement	٣,٨٦	–	-	-	*٠,٨٧٥-
After showing the third advertisement	٤,٧٣	–	–	–	–

Table (4): Illustrates the results of multiple comparisons between the mean scores of repeated measurements before and after exposure to short advertisements.
*Significant at the 0.05 level

It is evident from Table (4) the presence of statistically significant differences between the mean scores of measurements for the responses of the youth research sample according to pairwise comparisons. Differences are observed between the measurements before and after exposure to short advertisements, indicating the significant impact of the short advertisements in enhancing self-reported behavioral changes regarding virtual identity security among youth gradually.

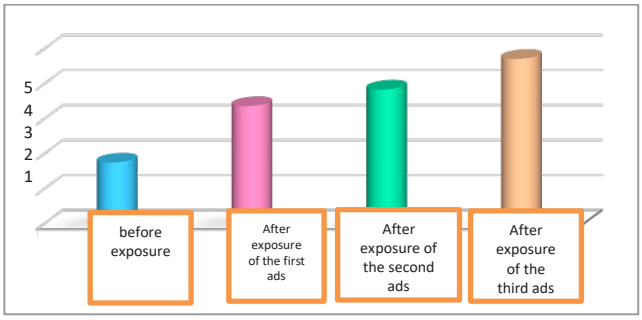


Figure (9): Illustrates the mean scores of measurements for self-reported behavioral changes regarding virtual identity security among youth gradually before and after exposure to short advertisements.

From Tables (3) and (4), and their results, along with Figure (9), it is evident that the second statistical hypothesis of the research is achieved.

17-3- Results of the Third Statistical Hypothesis:

The third hypothesis states that "there are statistically significant differences at a significance level (≥ 0.05) between the mean scores of responses of youth sample before and after exposure to short advertisements aimed at enhancing the general readiness for cybersecurity among the youth demographic."

To verify this hypothesis, the researcher used the "One Way Repeated-measured ANOVA" test and the "Bonferroni" test for multiple comparisons. Additionally, the researcher employed the Eta squared (ηp2) equation to calculate the effect size for the short advertisements. Cohen provided an interpretation for the "effect size" value, where it is considered small if its value is (0.01), medium if its value is (0.06), and large if its value is (0.14). The results are as follows:

Source of variance	Sum of squares	Degrees of freedom	Mean squares	F	Significance level	Eta square
Groups (repeated measures)	٤٥٠,٣٨	١,٨٤	٢٤٤,٣٩	٨٧٥,٨٠	٠,٠٠١	٠,٩٠٢
The error	٤٨,٨٥	١٧٥,٠٧	٠,٢٨			

Table (5): Presents the results of the One Way Repeated-measured ANOVA analysis for the mean scores of repeated measurements regarding the effect of short advertisements on enhancing the general readiness for cybersecurity among the youth demographic.
* Significant at the 0.05 level

It is evident from Table (5) that there are statistically significant differences between the mean scores of repeated measurements for enhancing the general readiness for cybersecurity among the youth demographic before and after exposure to short advertisements. The value of "F" was (875.80) with a significance level of (0.001), and the Eta squared value was (0.860), which is greater than the threshold of 0.14 defined by Cohen for a large effect size. This indicates that the short advertisements exposed to the research sample had a significant effect in enhancing awareness of cybersecurity among young people.

Groups (repeated measures)	SMA	Before showing the advertisements	After showing the first advertisement	After showing the second advertisement	After showing the third advertisement
Before showing the advertisements	١,٧٥	-	*١,٥٩٧-	*٢,١٦٣-	*٢,٩٥٦-
After showing the first advertisement	٣,٣٥	-	-	*-٥٦٦.-	*١,٣٥٩-
After showing the second advertisement	٣,٩٢	-	-	-	*٠,٧٩٣-
After showing the third advertisement	٤,٧١	-	-	-	–

Table (6) illustrates the results of the Bonferroni test for multiple comparisons to determine the directions and significance of differences between the mean scores of repeated measurements before and after exposure to short advertisements.

It is evident from Table (6) that there are statistically significant differences between the mean scores of repeated measurements for the responses of the youth research sample according to pairwise comparisons. Differences between repeated measurements before and after exposure to short advertisements are observed, indicating the significant impact of the short advertisements in gradually enhancing the general readiness for cybersecurity among the youth demographic. Figure (3) illustrates this.

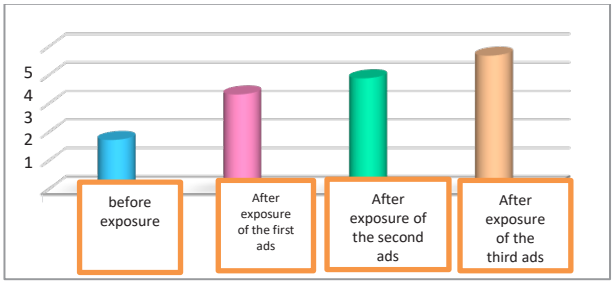


Figure (10): Illustrates the mean scores of repeated measurements for enhancing the general readiness for cybersecurity among the youth demographic gradually before and after exposure to short advertisements.

The achievement of the third statistical hypothesis of the research is evident from Tables (5) and (6) and their results along with Figure (10).

18- Conclusion

The statistical results of the research indicate that short video advertisements aimed at raising awareness about virtual identity security and displayed on the YouTube platform have contributed to increasing the average scores of repeated measurements of responses among the youth sample in raising awareness about virtual identity security. Additionally, they have had an impact on enhancing self-reported behavioral changes regarding virtual identity security among youth, which in turn has stimulated a general readiness for cybersecurity within the youth demographic.

19- References

- Allison, Stuart F. H., Amie M. Schuck, and Kim Michelle Lersch. 2005. ‘‘Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim=Offender Characteristics.’’ Journal of Criminal Justice 33:19–29 [Accessed:11 May 2023].
- Applegate, S. (2009), “Social engineering: hacking wetware!”, Information Security Journal: A Global Perspective, Vol. 18 No. 1, pp. 40-46, [Accessed from: Business Source Complete].
- Bossler, Adam M. and Thomas J. Holt. 2009. ‘‘On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory.’’ The International Journal of Cyber Criminology 3:400–420 [Accessed:22 July 2023].
- Chander Mohan Gupta and Devesh Kumar (2020): Identity theft: a small step towards big financial crimes, Journal of Financial

Crime, Vol. 27 No. 3. DOI 10.1108/JFC-01-2020-0014 [Accessed:18 July 2023].
- Chawki M. and Abdel Wahab M. S. (2006): Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol.11 n°1 [Accessed:21 January 2023].
- Choi, Kyung C. 2008. ‘‘Computer Crime Victimization and Integrated Theory: An Empirical Assessment.’’ International Journal of Cyber Criminology 2:308–333 [Accessed:21 January 2023].
- Chu, Bill, Thomas J. Holt, and Gail Joon Ahn. 2010. Examining the Creation, Distribution, and Function of Malware On-Line. Technical report for National Institute of Justice. NIJGrant No. 2007-IJ-CX-0018 [Accessed:14 June 2023].
- Cole, S.A., & Pontell, H. (2006). Don't below hanging fruit: identity theft as moral panic. In T. Monahan (Ed.), Surveillance and security (pp. 125í147). London: Routledge [Accessed:5 May 2023].
- Computer Security Institute. 2009. Computer Crime and Security Survey. Available at (http://www.cybercrime.gov/ FBI2008.pdf) (accessed June 5, 2010).
- Eszteri D. & Máté I. M. (2016): Identity Theft in the Virtual World: Analysis of a Copyright Crime in Second Life from the Perspective of Criminal Law and IT Forensics [Accessed:18 July 2023].
- Finn, Jerry. 2004. ‘‘A Survey of Online Harassment at a University Campus.’’ Journal of Interpersonal Violence 19:468–483. [Accessed:18 July 2023].
- Furnell, Steven. 2002. Cybercrime: Vandalizing the Information Society. Boston, MA: Addison-Wesley. Garmezy, N. 1985. ‘‘Stress-Resistant Children: The Search of Protective Factors.’’ Pp. 213–233 in Recent Research in Developmental Psychopathology, edited by J. E. Stevenson. New York: Pergamon Press. [Accessed:5 March 2023].
- Goodin, Dan. 2007. ‘‘TJX Breach was Twice as Big as Admitted, Banks Say.’’ The Register. Available at (http:// www.theregister.co.uk/2007/10/24/tjx_breach_estimate_grows/) (accessed October 23, 2008) [Accessed: 5 April, 2023].
- Gupta, Mohan C., Devesh K. (2020): Identity theft: a small step towards big financial crimes, Journal of Financial Crime; London Vol. 27, Iss. 3, DOI: 897-910. DOI:10.1108/JFC-01-2020-0014
- Hogan, B. (2010). *The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. Bulletin of Science, Technology & Society, 30(6), 377–386.* doi:10.1177/0270467610385893
- Holt, T. J., & Turner, M. G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. Deviant Behavior, 33(4), 308–323. doi:10.1080/01639625.2011.584050
- Holt, Thomas J. and Adam M. Bossler. 2009. ‘‘Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization.’’ Deviant Behavior 30:1–25.
- Holt, Thomas J. and Eric Lampke. 2010. ‘‘Exploring Stolen Data Markets On-Line: Products and Market Forces.’’ Criminal Justice Studies 23:33–50 [Accessed:14 June 2023].**https://www.aura.com/learn/how-does-identity-theft-happen#3.-Lost-or-stolen-phones-and-digital-devices** [Accessed:5 May 2023].
- Irvin-Erickson Y., Ricks A. (2019*).* Identity theft and fraud victimization: What we know about identity theft and fraud victims from research-and practice-based evidence. https://victimresearch.org/research/research-syntheses/[Accessed:18 July 2023].
- Jougleux P. (2012): Identity theft and internet, Int. J. Liability and Scientific Enquiry, Vol. 5, No. 1. [Accessed: 2 June, 2022].
- Marchini, K., & Pascual, A. (2019). 2019 fraud study: Fraudsters seek new targets and victims bear the burnt. https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-reportfraudsters-seek-new-targets-and-victims-bear-brun [Accessed: 14 th March, 2023].
- Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. Mediterranean Journal of Social Sciences. doi:10.5901/mjss.2016.v7n3s1p135
- Nazario, Jose. 2003. Defense and Detection Strategies against Internet Worms. Boston, MA: Artech House [Accessed: 5 April, 2023].

- Newman, Grame and Ronald Clarke. 2003. Superhighway Robbery: Preventing E-Commerce Crime. Cullompton: Willan Press
- Randa, R., & Reyns, B. W. (2019). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. Deviant Behavior, 4, 1–15 [Accessed: 5 April, 2023].
- Subrahmanyam, K., & Šmahel, D. (2010). Constructing Identity Online: Identity Exploration and Self-Presentation. Advancing Responsible Adolescent Development, 59–80. doi:10.1007/978-1-4419-6278-2_4 [Accessed: 18 April, 2023].
- Symantec Internet Security Threat Report: Trends for January- June 06. [online]. Available from: http://www.symantec.com/business/threatreport/archive.jsp [Accessed: 22 April, 2023].
- Szor, Peter. 2005. The Art of Computer Virus Research and Defense. Upper Saddle River, NJ: Addison Wesley [Accessed: 11 June, 2022].
- Taylor, Robert W., Eric J. Fritsch, John Liederbach, and Thomas J. Holt. 2010. Digital Crime and Digital Terrorism, 2nd edition. Upper Saddle River, NJ: Pearson Prentice Hall [Accessed:6 January 2023].
- Wall, David S. 2007. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press [Accessed: 22 April, 2023].
- Wang, B. S. K., & Huang, W. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet. Internet Journal of Criminology. Symantec Corporation. [Accessed:6 July 2023].
- Yar, M., & Steinmetz, K. F. (2019): Cybercrime and Society, 3rd Edition, SAGE Publications Ltd, ISBN 9781526481658 [Accessed:6 July 2023].

Section: Awareness Levels							
Team No.	Title	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	References
1	I agree that I have a clear understanding of what virtual identity security entails.						(Krugera & Kearney 2006)
2	I agree that I am aware of the potential risks associated with sharing personal information online.						
3	I agree that I can identify common tactics used by cybercriminals to compromise virtual identities.						
4	I agree that I am conscious of the importance of using secure passwords for my online accounts.						
5	I agree that I understand the significance of regularly updating my privacy settings on social media platforms.						
6	I agree that I am aware of the potential consequences of falling victim to online identity theft.						
7	I agree that I have knowledge of how to recognize and avoid phishing attempts targeting virtual identities.						
8	I agree that I am conscious of the importance of multi-factor authentication for enhancing virtual identity security.						
9	I agree that I am well-informed about the vulnerabilities associated with virtual identity in online environments.						
10	I agree that I am aware of the steps to take in case my virtual identity is compromised.						
Section: Self-Reported Behavior Changes							
1	I agree that I have made changes to my password practices (e.g., using stronger passwords, changing them regularly) after learning about virtual identity security.						
2	I agree that I have become more cautious about sharing personal information online due to awareness of virtual identity security risks.						
3	I agree that I now actively review and update privacy settings on my social media accounts.						
4	I agree that I have started using two-factor authentication for my online accounts as a result of increased awareness about virtual identity security.						
5	I agree that I am more vigilant about recognizing and avoiding potential phishing attempts.						
6	I agree that I have reduced the amount of personal information shared on public platforms or websites.						
7	I agree that I now regularly monitor my online accounts for any unusual or unauthorized activities.						
8	I agree that I am more cautious about the websites and applications I use to ensure they are secure.						
9	I agree that I have changed my online behavior to limit the use of public Wi-Fi networks for sensitive activities.						
10	I agree that I have become more proactive in educating friends and family about virtual identity security practices.						

Measurement adopted from (Krugera & Kearney 2006) on the 5-Point Likert scale :Appendix (1)

Table 4: appendix (1)