International Journal of Information Security
https://doi.org/10.1007/s10207-024-00824-0

REGULAR CONTRIBUTION

Is cyber hygiene a remedy to IPTV infringement? A study of online streaming behaviours and cyber security practices

Rajiv Shah[1,2] · Deniz Cemiloglu[2] · Cagatay Yucel[2] · Raian Ali[3] · Vasilis Katos[2]

Abstract
Spurred by the rapid modernisation of the sector and the advent of Internet Protocol Television (IPTV), audiovisual (AV) piracy is at epidemic levels, with interventions having limited effect. To date, the dominant themes in interventions have been around personal deterrence (i.e. the threat of legal action) and have not considered other factors that may influence an individual's decision to consume infringing content. In this paper, we consider psychological factors, including perceptions around risk-taking, security behaviours, problematic internet use and personality traits, to gain a comprehensive understanding of factors influencing engagement with IPTV and the potential implications for cyber security. For this purpose, a survey was conducted with 283 participants living in the UK (age range 18–74, male 104), and an integrated structural equation model was constructed. Our findings showed a positive relationship between security behaviours and the perceived risk of viewing IPTV and a negative relationship between the dark personality triad and the perceived risk of viewing IPTV. They suggest that security behaviours fully mediate the relationship between problematic internet use and IPTV risk-taking, indicating a potential new path for anti-piracy interventions with greater efficacy.

Keywords Internet protocol television · Dark personality triad · Problematic internet use · Human aspects of cyber security · Risk taking · Piracy · Copyright infringement

1 Introduction

In studies conducted by the EU Intellectual Property Office (EUIPO) and the Audiovisual Anti-Piracy Alliance (AAPA), it was revealed that trends in illegal Internet Protocol Television (IPTV) streaming practices are steadily increasing [1, 2]. Despite the introduction of recent legislation and substantial efforts by national and Pan-European law enforcement to combat piracy [3, 4], and their successes in dismantling prominent criminal groups, AV piracy does not seem to subside. Organised criminal groups operate over a variety of business models—ranging from free services to formal monthly subscriptions, with the underlying infrastructure commoditised and resold, making direct enforcement actions difficult due to the disaggregated nature [1].

In this study, we focus on consumer behaviour and explore the factors that influence one's decision to consume potentially infringing AV content online through IPTV services. This study aims to identify potential factors that contribute to the behaviour of consuming infringing content and as such, identify areas of intervention that are likely to have a positive impact.

The theoretical background and literature review on motivators towards AV piracy are presented in the following section, with associated hypotheses being derived. With the context from the literature review, we then construct an operational model. Then, for the purpose of this study, we introduce and validate a means of measuring IPTV viewing risk, which adopts well-accepted risk perception and risk-taking approaches. The newly introduced scale is combined

✉ Vasilis Katos
vkatos@bournemouth.ac.uk

Rajiv Shah
rajiv.shah2@kellogg.ox.ac.uk

Deniz Cemiloglu
dcemiloglu@bournemouth.ac.uk

Cagatay Yucel
cyucel@bournemouth.ac.uk

Raian Ali
raali2@hbku.edu.qa

[1] University of Oxford, Oxford, UK

[2] Bournemouth University, Poole, UK

[3] Hamad Bin Khalifa University, Ar-Rayyan, Qatar

Published online: 06 March 2024

with the other identified constructs in a fully estimated structural equation model. The paper concludes with a discussion of the findings and potential implications of the study.

2 Theoretical background

Several factors can influence the decision to consume AV content through third-party sites. It has been reported that risky online behaviour can be predicted by risk perception [5–7], cyber security knowledge, risk-taking in real life and the individual's personality traits [8].

2.1 Risk perception

Perceived risk is defined by [9] as the subjective assessment by an individual of the potential uncertainties and negative consequences linked to a decision or action. When faced with risky decisions, people tend to prioritise avoiding mistakes rather than maximising gains [10], making perceived risk a significant factor explaining behaviour in decision-making contexts. In the context of online piracy, perceived risk encompasses various elements, including the chance of getting caught and the severity of potential consequences if caught. Perceived risk can be measured to be high for certain threats and activities such as identity theft, viruses, phishing and keylogger attacks but low for general internet browsing and information sharing on social media [11]. Existing research has consistently demonstrated that perceived risk significantly influences people's intentions regarding digital piracy [5–7]. However, the relationship between perceived risk and risk-taking in online piracy is complex. While it is argued that the relationship between risk perception and risk-taking is expected to be negative and high-risk perception will lead to low risk-taking, it has been reported that individuals may perceive and respond to risks in different ways depending on the situation and their personal characteristics and experiences, leading to potentially paradoxical attitudes towards risk. Kotchick et al. [12] argued that the inconsistent findings regarding the relationship between risk perception and risk-taking can be conceptually explained to some extent. For instance, being aware of engaging in risky activities can increase the sense of personal risk, leading to a positive correlation. Conversely, a reduced sense of vulnerability can contribute to higher risk-taking, resulting in a negative correlation. The latter is also supported by [13].

Against the above, we adopt the more rational and intuitively straightforward hypothesis of the two:

H 1 There is a negative relationship between perceived risk and risk-taking regarding the viewing of IPTV content.

2.2 Cyber hygiene

Cyber hygiene refers to the adaptive knowledge and behavio urs aimed at mitigating the risks associated with online activities, which can jeopardise an individual's social, financial, and personal information [14]. Cyber security awareness is a key driver of cyber security behaviour and is defined as an individual's understanding of the importance of information security, their responsibilities, and the behaviour they exhibit in relation to safeguarding information by [15]. Studies show that cyber security awareness plays a vital role in promoting security behaviour [16, 17] and adoption of cyber hygiene practices [18]. For example, Li et al. [19] investigated the impact of cyber security policy awareness on employees' behaviour and found that when employees are aware of their company's security policy and procedures, they are more able to positively complete cyber security tasks than those who are not aware. Moreover, Jaeger and Eckhardt [20] showed that situational information security awareness increases perceived threat and perceived coping efficacy (i.e. the belief that one can effectively cope with a challenging situation) and, ultimately, actual behavioural responses to phishing attacks. The research on the impact of security behaviours on digital piracy is relatively sparse, instead with more research present on known security impacts of IP infringement—i.e. the potential to be infected with viruses and malware [21–23].

Based on the above discussion, we hypothesise that:

H 2 Users who apply cyber hygiene practices (security behaviours) tend to perceive higher risks associated with viewing IPTV content.

2.3 Problematic internet Use

Problematic Internet usage is described as an individual's lack of control over their internet activities, leading to disruptions in meeting social, work, and personal obligations by Young [24]. Studies have investigated the connection between problematic internet use and security behaviours, revealing a statistically significant correlation between symptoms associated with a negative relationship with the internet and risky behaviour online [25, 26]. Deutrom et al. [27] expanded on this relationship, using Jessor's Problem-Behaviour Theory (1977) to justify this link and relate it to the ongoing COVID-19 pandemic. Moreover, recent research in "problematic video streaming" indicated a positive relationship with problematic internet use [28–30]. Accordingly, we constructed the following two hypotheses introducing the mediating role of cyber security behaviour between problematic internet use and risk-taking in viewing IPTV content:

H 3 There is a negative relationship between Problematic Internet Use and cyber security practices.

H 4 There is a negative relationship between cyber security practices and risk-taking for viewing IPTV content.

2.4 Personality traits

Personality traits are seen as factoring into decisions by people to commit IP infringement in multiple studies, with Ming et al. (2015) and Satchell et al. (2022) finding evidence of correlation between IP infringement and the big five personality traits (Digman 1990) and the triarchic model of psychopathy (Patrick et al. 2009), respectively. For IP infringements in particular, Satchell et al. [31] conducted two comprehensive studies focusing on psychopathic traits, reporting that low self-control (Disinhibition and Conscientiousness) is a predictor of media piracy. Machiavellianism was identified as a partially supporting factor to IP infringement by [32], which would be interesting to explore further, since it was identified as a predictor of attitude to piracy by Al-Rafee and Cronan [33]. The dark personality traits have been studied in the context of risk and IPTV streaming. The dark triad comprises three negative personality traits associated with harmful behaviours: Machiavellianism, characterised by a manipulative view of human nature; narcissism, featuring grandiose self-importance and a need for admiration; and psychopathy, defined by a lack of empathy and a tendency for impulsive and antisocial behaviour [34]. Dark traits have been shown to be positively related to risky behaviour [35, 36], as well as addictive behaviour [37]. Hosker-Field et al. [38] studied the interplay between psychopathy, risk perception and risk-taking and found that some psychopathy traits were related to risk-taking via risk perception. Assuming that a high-scoring dark trait will be more likely to engage in risk-taking activity, in our case stream content despite the associated cyber security risks, the following hypothesis is formulated:

H 5 There is a negative relationship between dark personality traits and the perceived risk of viewing IPTV content.

The above hypothesis is constructed assuming that perceived risk fully mediates the (positive) relation between dark traits and the viewing of IPTV content.

The hypotheses of this research are summarised in the operational model presented in Fig. 1.

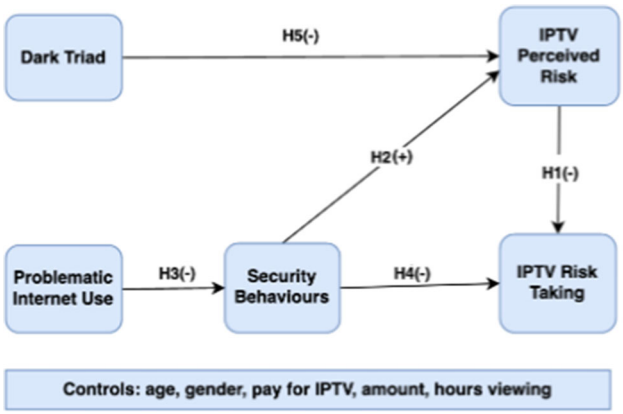

Fig. 1 The operational model

3 Method

3.1 Participants

The primary data for this study were collected on 22 April 2022 and the questionnaire was administered through Prolific.[1] Solely participants resident in the UK were chosen to retain consistency since streaming services available differ across countries, and there may be certain cultural and legal factors that impact people's decisions. Compensation for participation in the questionnaire was reimbursed through Prolific, subject to meeting the criteria that no more than one attention check was failed, out of three. Excluding the failed attention checks, and incompletely filled questionnaires, a total number of 283 fully answered questionnaires were returned, with the demographics of the respondents shown in Table 1.

3.2 Measures

The measures used in this research are based on the cited literature. A five-point Likert scale was used for all structural items, except for the risk constructs, where a seven-point scale was adopted, following the specification of the DOSPERT scale. The risk constructs consist of targeted questions for both perceived risk, and risk-taking specific to IPTV viewing. The following measures were used or developed:

Security behaviours To measure the participant's alignment to generally established security practices, the Human Aspects of Information Security Questionnaire (HAIS-Q) [39] was utilised. This was chosen instead of the Cybersecurity Judgment Questionnaire [40] since it offered the capacity to analyse multiple component domains. It has also been validated by multiple studies, increasing confidence in the integrity of the scale [41]. The scale measures knowledge, intention, and behaviour across seven security domains: password management, email use, internet use, social networking use, incident reporting, mobile computing, and information handling.

For our study, three domains overall were used: password management, internet use, and social networking use. These

[1] https://prolific.co.

Table 1 Sample demographics

	Frequency	Percentage
Gender		
Male	104	36.749
Female	174	61.484
Non-binary	5	1.767
Age		
18–30	98	34.629
31–40	78	27.562
41–50	49	17.314
51–60	42	14.841
60	16	5.654
IPTV subscription		
No	38	13.428
Yes	245	86.572
Subscription amount		
< 20	129	45.583
20–40	84	29.682
40–60	21	7.420
60–80	5	1.767
80	6	2.449
Hours of viewing		
< 25	72	25.442
25–50	58	20.495
50–75	64	22.650
75–100	30	10.601
>100	59	20.848

$N = 283$

were selected because they hold the closest association to the subject matter of IPTV infringement, as opposed to incident reporting, information handling and others that are not directly relevant. The HAIS-Q also tests multiple areas of security behaviours through knowledge of policy, attitudes to policy and self-reported behaviour. Again, in the context of this study, knowledge of policy and attitudes to it can be deemed largely irrelevant since it is the behaviour for each of the domains that have been found to hold statistical significance and, as such, were removed. The overall Cronbach's α for the self-reported behaviour section utilised was $\alpha = 0.526$. Although this was lower in our survey compared to other studies where the alphas for the HAIS domains ranged from 0.76 to 0.83 [42] we will proceed with the analysis, as HAIS-Q is a fairly mature scale and all other sections of the study have an acceptably high alpha.

Problematic Internet Use Existing literature utilised the Online Cognition Scale to determine problematic patterns of internet usage [25], but for this study, it was discounted due to the length and depth of the scale, in which a total of 36 individual points were required. The time required to complete

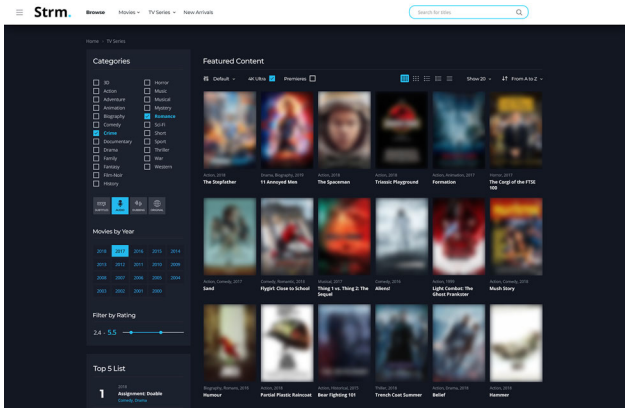

Fig. 2 The baseline site mock-up. The blurring within the figure was intentional to avoid unintended copyright infringement

the questionnaire was a vital factor to ensure that participants remained engaged in the activity. As a result, the Problematic Internet Use Questionnaire (PIUQ-SF-6) was utilised instead [43]. Consisting of solely 6 questions, it is a condensed version of the original 30-item survey [44] retaining the three subscales (obsession, neglect and control disorder), and has been confirmed as a robust scale ($\alpha = 0.82$). This finding is in agreement with Cronbach's alpha calculations from other studies ($\alpha = 0.87$ [43], $\alpha = 0.80$ [45])

Dark personality traits The dark personality triad scale or SD3 [34] is a second-order construct of 27 items contributing to three subscales of narcissism (self-importance to the degree empathy for others is diminished, $\alpha = 0.71$), Machiavellianism (manipulative behaviour and disregard of morality and ethics, $\alpha = 0.77$) and psychopathy (lack of empathy and emotional response, along with detachment from behaviours, $\alpha = 0.80$). This finding is in agreement with Cronbach's alpha results reported by the authors of the measure (Machiavellianism $\alpha = 0.76$, Psychopathy $\alpha = 0.73$, Narcissism $\alpha = 0.78$ [34]).

IPTV viewing (perceived risk, risk-taking) The approach for developing IPTV-specific risk measures included the development of seven hypothetical scenarios, with ordered cyber threat levels based on a mock-up of an IPTV streaming site. The baseline mock-up case is shown in Fig. 2 and contains no indications that copyright may be potentially infringed, instead, being described as a free streaming service.

To obtain the mock-up, a template for a streaming website was purchased from an online resource marketplace. Using the template and randomly selected posters of movies and TV shows, a draft was created. The posters were intentionally blurred to avoid infringing on copyrights, and also to ensure that the design of the website retained prime focus. Attention is intended to be drawn towards the left-hand side with options to filter content, emulating aggregation sites [46,

47] and implying that there is a practically unlimited amount of content on the site, as would be the case with an infringing site due to the absence of restrictions around rights and distribution [48].

With the mock-up created, the next stage was to place it in a variety of plausible scenarios, in which the potential risk of the action is different. This was achieved by researching common malicious features present on websites and implementing equivalents on the mock-up [49, 50]. This process allowed for the creation of seven distinct scenarios as summarised in Table 2. All the scenarios and their representative nature of the common malicious features were face-validated with both an ordinary user and a domain expert.

Pop-up ad Utilising an invasive pop-up advertisement with a suspicious call-to-action, claiming that the user has won a prize is a hallmark of malicious advertisements (also known as malvertising) and is documented in literature as both being common on sites aiding IP infringement, and a common method malicious actors employ to attempt to gain a foothold [51, 52].

Banner ad Utilising banner ads alongside content with aggressive calls-to-action is known to be a tactic that malicious actors use when exploiting advertising networks to deliver malware. It has been observed that when users notice adverts of this type that their confidence in websites decreases, which may cause them to question the legitimacy of the mock-up site [53–55].

Spyware User attitudes to spyware are well documented, ranging from the "I have nothing to hide" argument to severe concerns. As a result, it makes sense to isolate this as a potential factor impacting a user's choice to utilise the site. Encountering spyware while browsing the web is not outside the realm of possibility, especially on websites that have a history of hosting infringing content [56–58].

Ransomware An increasingly prevalent type of malware, ransomware is opposite in its behaviour compared to spyware. Instead of sitting quietly in the background, it immediately destroys data, creating a direct impact shortly after infection. As a result, even users with a sense of apathy towards malware (i.e. the "nothing to hide" argument) may be inclined to avoid a service that carries the risk of infecting with ransomware and, in turn, disrupting their activities [59–61].

Install app Requiring an application installation to access content is known to discourage users from utilising a website or service and, as a result, may discredit it. In the context of malicious actors, this has been observed as a tactic to gain access to a user's device before progressing further, making the interaction something that a user may be aware to look out for, impacting their choice [62–65].

The scenarios were presented to the survey participants by initially showing them the control scenario, followed by the six remaining scenarios presented in a random order. The scenarios were attached to the two seven-point scales to record perceived risk and risk-taking, following the convention used by the DOSPERT scale (Fig. 3). For each of the scenarios, the following two questions were asked, therefore totalling 14 questions:

- *Risk perception* People often see some risk in situations that contain uncertainty about what the outcome or consequences will be and for which there is the possibility of negative consequences. However, riskiness is a very personal and intuitive notion, and we are interested in your gut-level assessment of how risky each situation or behaviour is. Please indicate how risky you perceive the situation. Provide a rating from 'Not at all Risky' to 'Extremely Risky'.
- *Risk-taking* Please indicate the likelihood that you would use this service if you were to find yourself in that situation. Provide a rating from 'Extremely Unlikely' to 'Extremely Likely', using the following scale.

Table 3 presents the results of an exploratory factor analysis (EFA) for the developed IPTV risk items. For the EFA, 75 responses were randomly selected from the sample. The alphas were acceptably high (over 0.7) for both measures, showing adequate internal consistency. The analysis indicates two factors, grouping scenarios 1, 2, 3, 6, 7 in one factor and 4, 5 in another. For both measures, all items produced loadings greater than 0.4, with no cross-loadings over this threshold. The Kaiser–Meyer–Olkin values were above 0.6, showing that the dataset can be considered for factor analysis. Bartlett's test showed no correlation between the variables.

3.3 Consistency, validity and reliability of the survey instrument

As the questionnaires used in this research are validated and widely accepted in the literature, we argue that content validity is supported (Straub, 1989). However, as the IPTV constructs are newly introduced, validation was performed for the purpose of this research. In addition to the validity and reliability tests performed for all constructs, the IPTV items were subject to additional exploratory factor analysis as shown above. In addition, the first order factors were used in the final estimated model. Creation of sub-constructs and second order factors for IPTV viewing would result in the creation of another domain specific measure and is reserved for future research. In any case, the IPTV viewing measures adopted the DOSPERT scale approach.

Against the above, confirmatory factor analysis (CFA) to examine the properties of first and second order dimensions was performed, with the loadings summarised in Table 4. All components showed acceptably high loadings, though

Table 2 Mock-up scenarios

#	Scenario name	Description	Question preamble	Expected threat /risk level
1	Control	Baseline mock-up as is	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up*) There are no limits on access to the content.	Very Low
2	Pop-up ad	With intrusive pop-up advert	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up with pop-up ad banner*). There are no limits on access to the content.	Low-Medium
3	Banner ad	With multiple banner adverts on the sides of the content	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up with fixed ad banners on the main web page*). There are no limits on access to the content.	Medium
4	Spyware	Will steal passwords but leaves it operable	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up*). By accessing the site, there is a **chance** of being infected with a virus (spyware) that will steal your passwords and other sensitive information on your computer **but will otherwise leave it operable.**	High
5	Ransomware	Will destroy information leaving computer inoperable	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up*). By accessing the site, there is a **chance** of being infected with a virus (ransomware) that will render everything on your computer unreadable, meaning you **cannot use the computer unless you pay a ransom**, and may lose all your files.	Very High
6	Install app to use	Requiring installation of player application	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up, with "STRM Content Player" software installation pop-up*) To access the content on the site, you need to **install** the "TRM Content Player" onto your computer.	Medium-High
7	Unable to verify license	Unsure if allowed to provide content in the UK legally	You have access to a portal with all TV content in the world accessible for free. It may look something like this. (*baseline mock-up*). We were not able to verify the site's license to provide content.	Medium

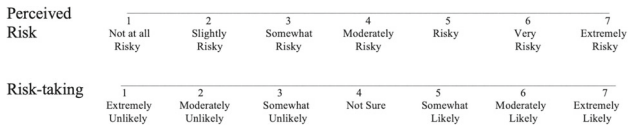

Fig. 3 The scales used for perceived risk and risk-taking, for viewing IPTV content

the first item of the dark personality triad, the Machiavelli subscale, had an unacceptably low loading (0.266) and was removed. The second-order loading of the scale, however, was acceptably high (0.777).

Table 5 summarises the properties and indices of the constructs. Most Cronbach alphas are close to, or over 0.7 (particularly the main constructs), which supports internal consistency [66]. For all constructs, the total variance explained (TVE) is above the 50% threshold, supporting instrument construct validity. The composite reliability (CR) values are higher than 0.70, leading to an acceptable construct composite reliability [67]. Considering that the values of the Kaiser–Meyer–Olkin (KMO) measure are larger than 0.50 and Bartlett's test is significant ($p < 0.05$) for all constructs and sub-constructs, we accept that the data is significantly meaningful for further analysis and indicates that the data are suitable for structure detection [68]. All intra-correlation coefficients (ICC) have values much larger than 0.10, so, structural equation analysis is supported [69].

3.4 Normality tests

Table 6 summarises the properties of the constructs or establishing whether these follow the normal distribution. The approach involves calculating the mean, standard deviation, skewness, and kurtosis statistics for the constructs and the Shapiro–Wilk test to assess normality. Although there is no consensus on the cut-off values for skewness and kurtosis before non-normality becomes a problem, a common guideline suggests that data is considered normal if skewness ranges from −2 to +2 and kurtosis ranges from −7 to +7 [67].

From the calculated values, it can be observed that all constructs have skewness and kurtosis values well within the acceptable range. Moreover, according to the S-W test, security behaviours, SD3 and risk-taking follow the normal distribution, whereas PIU and perceived risk do not follow the normal distribution.

Table 7 displays the correlation coefficients between all the pairs of constructs used in the analysis, along with the square root of the average variance explained (AVE) for each construct. This was done to check if the constructs are distinct from each other (ensuring construct discriminant validity). The results show that the correlation coefficients are significantly different from unity, and they are lower than the square root of the AVE of each construct, indicating that the constructs are different from each other.

3.5 Common method bias

The investigation for the presence of common method bias was performed using Harman's single factor test [70]. By loading all items on one factor, we note that the first factor explains only 24.9% of the total variance. In addition, six factors are identified which were found to follow closely the five constructs proposed. As such, we conclude that a risk of common method bias is minimal.

4 Results

Table 8 shows the results of two models, the hypothesised model and Harman's single factor model. The hypothesised

Table 3 EFA results for IPTV perceived risk and risk-taking measures

Perceived risk of IPTV viewing (Cronbach's $\alpha = 0.827$)			Risk-taking for IPTV viewing (Cronbach's $\alpha = 0.742$)		
	Factor loadings			Factor loadings	
Item	Factor 1	Factor 2	Item	Factor 1	Factor2
Pop-up ad	0.741		Banner ad	0.693	
Control	0.718		Control	0.661	
Install app	0.682		License	0.609	
Banner ad	0.681		Pop-up ad	0.586	
License	0.577		Install app	0.551	
Ransomware		0.990	Ransomware		0.697
Spyware		0.472	Spyware		0.495
KMO test	0.795		KMO test	0.678	
Bartlett's test (p)	χ^2 : 183.427	df: 21 (0.000)	Bartlett's test (p)	χ^2 : 126.498	df: 21 (0.000)
Chi-squared test (p)	17.304	df: 8 (0.027)	Chi-squared test (p)	19.149	df: 8 (0.014)

The applied rotation method is varimax

Table 4 Results of the Confirmatory Factor Analysis for all constructs

Construct	1st order loadings	2nd order loadings	Construct	1st order loadings	2nd order loadings
Security behaviours			Dark personality (SD3) cont'd		
Password		0.566	Narcissist		0.714
HAISQ_1	0.793		SD3_10	0.706	
HAISQ_2	0.482		SD3_11	0.593	
HAISQ_3	0.684		SD3_12	0.701	
Internet		0.766	SD3_13	0.705	
HAISQ_4	0.810		SD3_14	0.693	
HAISQ_5	0.864		SD3_15	0.398	
HAISQ_6	0.345		SD3_16	0.551	
Social		0.797	SD3_17	0.546	
HAISQ_7	0.643		SD3_18	0.522	
HAISQ_8	0.581		Psychopath		0.805
HAISQ_9	0.752		SD3_19	0.652	
Problematic internet use			SD3_20	0.498	
Obsession		0.839	SD3_21	0.577	
PIUQ_2	0.896		SD3_22	0.678	
PIUQ_6	0.896		SD3_23	0.639	
Neglect		0.856	SD3_24	0.706	
PIUQ_1	0.800		SD3_25	0.400	
PIUQ_5	0.800		SD3_26	0.550	
Control		0.866	SD3_27	0.680	
PIUQ_3	0.860		IPTV perceived risk		
PIUQ_4	0.860		Control	0.762	
Dark personality (SD3)			Pop-up ad	0.787	
Machiavelli		0.777	Banner ad	0.787	
SD3_1	0.266		Spyware	0.595	
SD3_2	0.694		Ransomware	0.488	
SD3_3	0.622		Install app	0.695	
SD3_4	0.622		License	0.744	
SD3_5	0.511		IPTV risk taking		
SD3_6	0.716		Control	0.762	
SD3_7	0.647		Pop-up ad	0.749	
SD3_8	0.510		Banner ad	0.846	
SD3_9	0.549		Spyware	0.443	
			Ransomware	0.312	
			Install app	0.600	
			License	0.749	

$N = 283$

model is a CFA on all five constructs of the study, whereas the single factor model contains all items in one factor (construct).

From the results in Table 8, it is established that the hypothesised model is an acceptable fit, whereas the single factor model is a poor fit. Moreover, by comparing the Chi-square results of the two models, we get Δchi-square/Δ df = 101.6428. As this value is substantially higher than the critical value of 3.84 per degree of freedom, we can conclude that single respondent bias is limited, and the latent factors correspond to separate constructs [71].

4.1 Structural model

The final structural model results are summarised in Table 9, and the standardised estimated coefficients are presented visually in Fig. 4. From this table, we conclude that the final model presented in Fig. 4 is a good fit.

Table 5 Properties of constructs and sub-constructs

Construct	Sub-construct	# items	Cronbach's α	TVE (%)	CR	KMO*	ICC
Security behaviours		**3**	**0.526**	**51.4**	0.757	**0.570**	**0.526**
	Password	3	0.367	44.3		0.509	0.367
	Internet	3	0.484	50.7		0.502	0.484
	Social	3	0.341	43.9		0.542	0.341
Problematic internet use		3	**0.812**	**72.9**	0.890	**0.714**	**0.810**
	Obsession	2	0.754	64.0		0.500	0.436
	Neglect	2	0.436	80.3		0.500	0.754
	Control	2	0.644	73.9		0.500	0.644
SD3		3	**0.646**	**58.7**	0.810	**0.640**	**0.646**
	Machiavelli	8	0.774	40.2		0.805	0.774
	Narcissist	9	0.778	41.9		0.829	0.778
	Psychopath	9	0.760	36.6		0.831	0.760
IPTV Perceived risk		7	**0.828**	**54.0**	0.869	**0.819**	**0.828**
	Control	1	NA				
	Pop-up ad	1	NA				
	Banner ad	1	NA				
	Spyware	1	NA				
	Ransomware	1	NA				
	Install app	1	NA				
	License	1	NA				
IPTV risk taking		7	**0.784**	**50.8**	0.835	**0.793**	**0.784**
	Control	1	NA				
	Pop-up ad	1	NA				
	Banner ad	1	NA				
	Spyware	1	NA				
	Ransomware	1	NA				
	Install app	1	NA				
	License	1	NA				

*Bartlett's test significant ($p < 0.001$)

Table 6 Construct properties for normality assessment

	Security behaviours	PIU	SD3	IPTV perceived risk	IPTV risk taking
Mean	5.025	2.264	2.383	2.962	4.462
Standard dev	0.822	0.767	0.474	0.712	0.795
Skewness	−0.166	0.410	0.178	0.678	−0.229
Kurtosis	−0.145	−0.434	−0.066	0.444	−0.059
S-W test (p)	0.230	< 0.001	0.180	< 0.001	0.157

4.2 Discussion

Looking at the paths of the model, we observe the negative relationship between the dark personality triad and perceived risk of viewing IPTV (accepting H5). In addition, the Psychopathy trait dominates the other two (with a standardised coefficient of 0.759), agreeing with the observation by [31]. Although there is no clear consensus in the literature on the direction of relationship between perceived risk and risk taking, for this study a negative relationship was confirmed (accepting **H4**). While such a relationship can be considered the default choice when assuming that people are rational decision makers, this is not always observed in some cases, and particularly in situations with thrill seeking individuals

Table 7 Correlation coefficients and AVE for the constructs

Construct	Security behaviours	PIU	SD3	IPTV perceived risk	IPTV risk taking
Security behaviours	[0.717][a]				
PIU	−0.261**	[0.854]			
SD3	−0.061	0.092	[0.766]		
Perceived risk	0.198**	0.014	−0.155**	[0.735]	
Risk taking	−0.391**	0.087	0.109	−0.598**	[0.713]

[a] Square root of AVE
**Correlation is significantly different from unity at the 0.01 level (2-tailed)

Table 8 Fit indices for hypothesised and single factor models

Fit index	Critical value	Hypothesised model	Single factor model
Chi-square		362.411	1378.839
df		211	221
p	< 0.05	0.000	0.000
Normed chi-square	< 3 good fit 3–5 mediocre fit	1.7175	6.24
RMSEA	< 0.08	0.050	0.136
CFI	> 0.9	0.947	0.592
TLI	> 0.8	0.936	0.533

Table 9 The final structural model

Fit index	Critical value	Structural model
Chi-square		369.526
df		214.000
p	< 0.05	0.000
Normed chi-square	3 good fit 3–5 mediocre fit	1.727
RMSEA	< 0.08	0.051
CFI	> 0.9	0.945
TLI	> 0.8	0.935

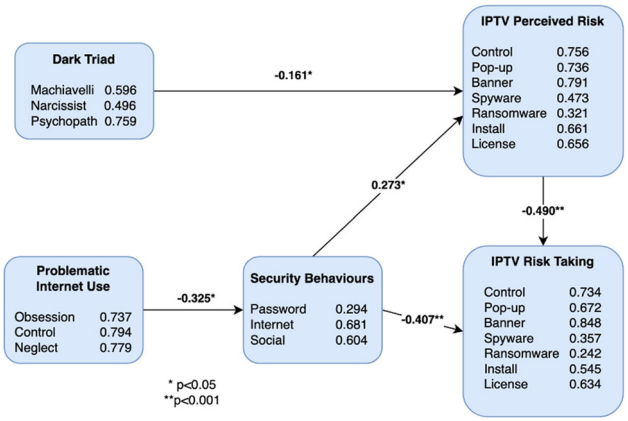

Fig. 4 The estimated model

who are prone to taking high risks to obtain high rewards [72, 73]. It should be noted however, that the highest risk-taking scenario, that of risk being infected by a ransomware as a "reward" of viewing AV content, shows the lowest weight.

The expected positive relationship between security beha viours and perceived (IPTV) risk further validates and confirms the model (accepting **H3**). Security behaviour has been shown to relate to risk perception [74], and risk perception has also been reported to be a predictor of security precautions [11].

Security behaviours mediate the relationship between problematic internet use and IPTV risk taking (accepting H1 and **H2**). Observing the path from digital addiction (PIU) to IPTV risk taking, we can establish that people with high internet addiction will be more willing to consume AV content (since the two negative estimates multiplied result to a positive number), at the expense of cyber security behaviours. The negative relationship between problematic internet use and cyber hygiene has been identified in several studies [25, 27, 75].

A summary of the hypotheses and their results is shown in Table 10.

Table 10 Hypotheses summary

Hyp.	Description	Result
H1	There is a negative relationship between perceived risk and risk taking regarding the viewing of IPTV content	Supported
H2	Users who apply cyber hygiene practices (security behaviours) tend to perceive higher risks associated with viewing IPTV content	Supported
H3	There is a negative relationship between Problematic Internet Use and cyber security practices	Supported
H4	There is a negative relationship between cyber security	Supported
H5	There is a negative relationship between the dark personality traits and perceived risk of viewing IPTV content	Supported

5 Implications

From the estimated model and the previous discussion, it can be seen that regardless of the introduction of legislation and enforcement actions being conducted to deter IPTV infringement, there will always be a market of viewers willing to consume AV content through unofficial, potentially copyright infringing means. This, in turn, will be a motivating factor for new actors to profit from infringing business models. Although most legislative controls focus on the providers of the infringing AV content and particularly those who receive financial gains, an attempt to tackle the consumer side to reduce the market size could also be a valid strategy, with additional potential benefits.

The medical research community generally accepts that there are certain behaviours that are governed by strong genetic influences [76] and that the physiology of the brain can determine some personality traits, psychopathy being one of them [77]. By adopting this view, it is deduced that individuals with a high dark personality score are less likely to change their behaviour, or at least observe a significant change, in AV consumption from potentially infringing websites.

With this said, it is acknowledged that problematic internet use and security behaviours can be improved with the provision of appropriate support. Internet addiction has been shown to be influenced by an individual's environment and can be a result of several factors, such as stressful life events [78], the recent COVID-19 lockdown [79], satisfaction with life [80], and coping style [81]. As such, tackling internet addiction would address IPTV streaming to an extent. It is important to caveat this however, in that interventions may not necessarily affect solely illegal streaming. Binge watching, for example, is an addictive behaviour that can appear in both legal and illegal AV content consumption.

The key differentiator and factor, according to our estimated model, is cyber security behaviours. The scientific literature has accumulated a considerable body of knowledge on cyber security awareness and training methodologies, approaches and practices (for example [82–84]). Cyber security awareness campaigns have been delivered in both corporate environments and to the wider public. Currently, the campaigns to fight IPTV crime focus on the well-being and prosperity of the creative industry, such as showcasing job losses, the impact on the theatre industry and so forth. We argue that if the narrative is updated to showcase the risks an average user may be facing when consuming infringing AV content, the seriousness of such actions will start being compared with risks in other potentially more important (to the user) areas such as online banking, personal data theft and so forth, leading to lower rates of infringement.

6 Conclusions, limitations and future work

In this paper, we explored the "nature versus nurture" perspective by examining psychology, risk-taking, and cyber security practices. Our findings indicate that people's inclination towards risk-taking, specifically in terms of viewing AV content with the risk of malware infection, is influenced by two main factors: dark personality traits and the level of digital addiction. Dark personality traits are generally considered stable over time, as they have genetic and biological components, making them less susceptible to change. On the other hand, digital addiction can be addressed through interventions aimed at promoting recovery.

Additionally, our research revealed that cyber hygiene, as observed through cyber security practices, acts as a mediating factor between digital addiction and risky IPTV viewing (risking malware infection). Therefore, to reduce the likelihood of individuals engaging in illegal IPTV consumption, we can target their digital addiction and/or improve their cyber security behaviour (and hygiene).

This suggests that anti-piracy campaigns focusing on security awareness can be an effective strategy. However, while these campaigns may contribute to a decrease in risky IPTV viewing practices, they may not completely eradicate the issue. There will always be a portion of the population that is prone to taking risks, and it is unlikely interventions will result in changes to such an outlook.

The research was a cross-sectional study conducted during a specific period (April 2022). Due to the nature of this problem domain, a longitudinal study would reveal more information, especially after deploying policies and campaigns targeting cyber security and illegal IPTV streaming.

The survey targeted the UK population. The survey would need to be expanded to cover more countries (the EU and the USA in particular) and be verified to ensure its findings align with studies that cover these areas.

This paper introduced a measurement scale for assessing risk in the IPTV domain. While the development of the scale followed the well-accepted DOSPERT scales, further validation is needed to ensure that the scale is aligned with and reflects the theoretical foundations of consumer behaviour in online AV content consumption.

Finally, the estimated structural equation model could be modified to use the dark personality triad as a moderating factor, as such factors are also found to influence (moderate) relationships rather than predicting outcome variables.

Acknowledgements The authors are indebted to Sheila Cassels and Mark Mulready from the Audiovisual Anti-Piracy Alliance (AAPA) for their great insights and support throughout this research. This work has been partially supported by IDEAL CITIES; a European Union's Horizon 2020 research and innovation staff exchange programme (RISE) under the Marie Skłodowska-Curie grant agreement No 778229.

Author Contributions RS developed the new risk scales and conducted data collection and analysis. DC and CY contributed to the development of the theoretical framework and selection of appropriate scales. RA and VK developed and tailored the research methodology (validation of new scales and confirmatory analysis) and supervised the implementation of the quantitative approach. All authors reviewed and edited the manuscript.

Data availability The dataset can be made available upon request.

Declarations

Conflict of interest Vasilis Katos is a member of the editorial board of the journal.

Ethical approval The data collection process adhered to Bournemouth University's ethical approval policy. Informed consent was obtained from all participants, and the collected data were anonymised prior to analysis.

References

1. Borghi, M., Katos, V., Ganarasvili, A., Favale, M., Mendis, D.: Illegal iptv in the european union: research on online business models infringing intellectual property rights-phase 3 (2019)
2. AAPA: Study on malware and audiovisual piracy highlights significant risks to european consumers. (2022)
3. Establishing the european electronic communications code
4. Directive (eu) 2019/790 of the european parliament and of the council of 17 april 2019 on copyright and related rights in the digital single market and amending directives 96/9/ec and 2001/29/ec (text with eea relevance.)
5. Liao, C., Lin, H.-N., Liu, Y.-P.: Predicting the use of pirated software: a contingency model integrating perceived risk with the theory of planned behavior. J. Bus. Ethics **91**(2), 237–252 (2010)
6. Yoon, C.: Theory of planned behavior and ethics theory in digital piracy: an integrated model. J. Bus. Ethics **100**(3), 405–417 (2011)
7. Pham, Q.T., Dang, N.M., Nguyen, D.T.: Factors affecting on the digital piracy behavior: an empirical study in Vietnam. Comput. Secur. **15**(2), 122–135 (2020)
8. Kennison, S.M., Chan-Tin, E.: Taking risks with cybersecurity: using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Front. Psychol. **11**, 546546 (2020)
9. Slovic, P.: Perception of risk. Science **236**(4799), 280–285 (1987)
10. Kahneman, D., Tversky, A.: Prospect theory: an analysis of decisions under risk. Econometrica **47**, 278 (1979)
11. van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P.: Risk perceptions of cyber-security and precautionary behaviour. Comput. Hum. Behav. **75**, 547–559 (2017)
12. Kotchick, B.A., Shaffer, A., Miller, K.S., Forehand, R.: Adolescent sexual risk behavior: a multi-system perspective. Clin. Psychol. Rev. **21**(4), 493–519 (2001)
13. Brewer, N.T., Weinstein, N.D., Cuite, C.L., Herrington, J.E.: Risk perceptions and their relation to risk behavior. Ann. Behav. Med. **27**(2), 125–130 (2004)
14. Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S., Hancock, G.M.: Holistic cyber hygiene education: accounting for the human factors. Comput. Secur. **92**, 101731 (2020)
15. Shaw, R.S., Chen, C.-C., Harris, A.L., Huang, H.-J.: The impact of information richness on information security awareness training effectiveness. Comput. Educ. **52**(1), 92–100 (2009)
16. Chen, C.C., Shaw, R., Yang, S.C.: Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Inf. Technol. Learn. Perform. J. **24**(1) (2006)
17. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., Basim, H.N.: Cyber security awareness, knowledge and behavior: a comparative study. J. Comput. Inf. Syst. **62**(1), 82–97 (2022)
18. Baraković, S., Baraković Husić, J.: Cyber hygiene knowledge, awareness, and behavioral practices of university students. Inf. Secur. J. Glob. Perspect. **32**(5), 347–370 (2023)
19. Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int. J. Inf. Manag. **45**, 13–24 (2019)
20. Jaeger, L., Eckhardt, A.: Eyes wide open: the role of situational information security awareness for security-related behavior. Inf. Syst. J. **31**(3), 429–472 (2021)
21. Watson, S., Zizzo, D., Fleming, P.: Determinants and welfare implications of unlawful file sharing: a scoping review. (2014)

22. Bosco, F., Shalaginov, A.: Identification and analysis of malware on selected suspected copyright-infringing websites. (2018)
23. Hsiao, L., Ayers, H.: The price of free illegal live streaming services. *arXiv preprint*, (2019)
24. Young, K.S.: Internet addiction: a new clinical phenomenon and its consequences. Am. Behav. Sci. **48**(4), 402–415 (2004)
25. Hadlington, L.: Human factors in cybersecurity: examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon **3**(7) (2017)
26. Aivazpour, Z., Rao, V.S.: Impulsivity and risky cybersecurity behaviors: a replication. (2018)
27. Deutrom, J., Katos, V., Ali, R.: Loneliness, life satisfaction, problematic internet use and security behaviors: re-examining the relationships when working from home during covid-19. Behav. Inf. Technol. **41**(14), 3161–3175 (2022)
28. Hasan, M.R., Jha, A.K., Liu, Y.: Excessive use of online video streaming services: Impact of recommender system use, psychological factors, and motives. Comput. Hum. Behav. **80**, 220–228 (2018)
29. Cheng, S.S., Chang, S.-L., Chen, C.-Y.: Problematic use of live video streaming services: Impact of personality traits, psychological factors, and motivations. In Proceedings of the 2019 8th International Conference on Software and Computer Applications, (Penang, Malaysia), p. 487–490. Association for Computing Machinery, (2019)
30. Rahat, M., Mojgani, J., Lethbridge, G., Al-Bya, H., Patterson, B., Bergmann, C.G., Van Ameringen, M.: Problematic videostreaming: a short review. Curr. Opin. Behav. Sci. **48**, 101232 (2022)
31. Satchell, L.P., Corr, P.J., Latzman, R.D.: Pirates with psychopathic personalities? The role of sub-clinical and normative traits in illegal streaming and downloading of media. J. Res. Personal. **96**, 104158 (2022)
32. Tjiptono, F., Arli, D.: Gender and digital privacy: examining determinants of attitude toward digital piracy among youths in an emerging market. Int. J. Consum. Stud. **40**(2), 168–178 (2016)
33. Al-Rafee, S., Cronan, T.P.: Digital piracy: factors that influence attitude toward behavior. J. Bus. Ethics **63**(3), 237–259 (2006)
34. Jones, D.N., Paulhus, D.L.: Introducing the short dark triad (sd3): a brief measure of dark personality traits. Assessment **21**(1), 28–41 (2014)
35. Crysel, L.C., Crosier, B.S., Webster, G.D.: The dark triad and risk behavior. Personality Individ. Differ. **54**(1), 35–40 (2013)
36. Maneiro, L., Navas, M.P., Van Geel, M., Cutrín, O., Vedder, P.: Dark triad traits and risky behaviours: identifying risk profiles from a person-centred approach. Int. J. Environ. Res. Public Health **17**(17), 6194 (2020)
37. Jauk, E., Dieterich, R.: Addiction and the dark triad of personality. Front. Psychiatry **10**, 662 (2019)
38. Hosker-Field, A.M., Molnar, D.S., Book, A.S.: Psychopathy and risk taking: examining the role of risk perception. Personal. Individ. Differ. **91**, 123–132 (2016)
39. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (haisq). Comput. Secur. **42**, 165–176 (2014)
40. Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E.: Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Comput. Hum. Behav. **84**, 375–382 (2018)
41. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The human aspects of information security questionnaire (hais-q): two further validation studies. Comput. Secur. **66**, 40–51 (2017)
42. McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., Pattinson, M.: Test-retest reliability and internal consistency of the human aspects of information security questionnaire (hais-q). In ACIS 2016 Proceedings, p. 56. (2016)
43. Demetrovics, Z., Király, O., Koronczai, B., Griffiths, M.D., Nagygyörgy, K., Elekes, Z., Tamás, D., Kun, B., Kökönyei, G., Urbán, R.: Psychometric properties of the problematic internet use questionnaire short-form (piuq-sf-6) in a nationally representative sample of adolescents. PLoS ONE **11**(8), e0159409 (2016)
44. Demetrovics, Z., Szeredi, B., Rózsa, S.: The three-factor model of internet addiction: the development of the problematic internet use questionnaire. Behav. Res. Methods **40**(2), 563–574 (2008)
45. Aivali, P., Efthymiou, V., Tsitsika, A.K., Vlachakis, D., Chrousos, G.P., Kanaka-Gantenbein, C., Bacopoulou, F.: Validation of the greek version of the problematic internet use questionnaire-short form (piuq-sf-6). EMBnet J. **26** (2021)
46. Lauinger, T., Kirda, E., Michiardi, P.: Paying for piracy? An analysis of one-click hosters' controversial reward schemes. In International Workshop on Recent Advances in Intrusion Detection, pp. 169–189. (2012)
47. Choi, S.-K., Kwak, J.: Feature analysis and detection techniques for piracy sites. KSII Trans. Int. Inf. Syst. (TIIS) **14**(5), 2204–2220 (2020)
48. Piotr, S., Danny, S.: Piracy of Digital Content. OECD Publishing, Berlin (2009)
49. Lee, S.J., Watters, P.A.: Gathering intelligence on high-risk advertising and film piracy: a study of the digital underground. Automat. Open Source Intell. pp. 89–102 (2016)
50. Manan, W.N.W., Ahmed, A.G.A., Kahar, M.N.M.: Characterizing current features of malicious threats on websites. in International Conference on Intelligent Computing & Optimization, pp. 210–218. Springer, (2018)
51. Abraham, S., Chengalur-Smith, I.: An overview of social engineering malware: trends, tactics, and implications. Technol. Soc. **32**(3), 183–196 (2010)
52. Nakerekanti, M., Narasimha, V.: Analysis on malware issues in online social networking sites (sns). in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 335–338. IEEE, (2019)
53. Liang, H., Xue, Y.: Avoidance of information technology threats: a theoretical perspective. MIS Quarterly, pp. 71–90. (2009)
54. Mansfield-Devine, S.: The dark side of advertising. Comput. Fraud Secur. **2014**(11), 5–8 (2014)
55. Masri, R., Aldwairi, M.: Automated malicious advertisement detection using virustotal, urlvoid, and trendmicro. In 2017 8th International Conference on Information and Communication Systems (ICICS), pp. 336–341. IEEE, (2017)
56. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., Konstan, J.: Stopping spyware at the gate: a user study of privacy, notice and spyware. In Proceedings of the 2005 Symposium on Usable Privacy and Security, pp. 43–52. (2005)
57. Gurung, A., Luo, X., Liao, Q.: Consumer motivations in taking action against spyware: an empirical investigation. Inf. Manag. Comput. Secur. **17**(3), 276–289 (2009)
58. Nyshadham, E.A., Ackerman, E., Rao, V.K.: Spyware–risk and ambiguity attitudes. Available at SSRN 2051045. (2012)
59. Sawler, D.R.: Ransomware: Psychological Warfare in the Cyber Realm. Utica College (2016)
60. Lévesque, F.L., Chiasson, S., Somayaji, A., Fernandez, J.M.: Technological and human factors of malware attacks: a computer security clinical trial approach. ACM Trans. Privacy Secur. (TOPS) **21**(4), 1–30 (2018)
61. Masuch, K., Hengstler, S., Schulze, L., Trang, S.: The impact of threat and efficacy on information security behavior: applying an extended parallel process model to the fear of ransomware. in Proceedings of the 54th Hawaii International Conference on System Sciences, p. 6691. (2021)

62. Milne, G.R., Labrecque, L.I., Cromer, C.: Toward an understanding of the online consumer's risky behavior and protection practices. J. Consum. Aff. **43**(3), 449–473 (2009)
63. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security, pp. 1–16. (2012)
64. Egelman, S., Felt, A.P., Wagner, D.: Choice architecture and smartphone privacy: There's a price for that. in The Economics of Information Security and Privacy, pp. 211–236. (2013)
65. Lévesque, F.L., Nsiempba, J., Fernandez, J.M., Chiasson, S., Somayaji, A.: A clinical study of risk factors related to malware infections. in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 97–108, Association for Computing Machinery, Berlin, Germany (2013)
66. Nunnally, J.C.: Psychometric Theory. McGraw-Hill, New York (1978)
67. Hair, J., Black, W.C., Babin, B.J., Anderson, R.E.: Multivariate Data Analysis, 7th edn. Pearson Educational International, Upper Saddle River, New Jersey (2010)
68. Kaiser, H.F.: An index of factorial simplicity. Psychometrika **39**(1), 31–36 (1974)
69. Kozlowski, S.W., Klein, K.J.: A Multilevel Approach to Theory and Research in Organizations: Contextual, Temporal, and Emergent Processes, vol. 3. Jossey-Bass, Hoboken (2000)
70. Harman, H.H.: Modern Factor Analysis. University of Chicago Press, Chicago (1967)
71. Brown, T.A.: Confirmatory Factor Analysis for Applied Research. The Guilford Press, London (2015)
72. Sarshar, M., Farley, F., Fiorello, C.A., DuCette, J.: T behaviour: psychological implications of thrill-seeking/risk-taking. Curr. Psychol. 1–8. (2019)
73. Lupton, D., Tulloch, J.: "Life would be pretty dull without risk": voluntary risk-taking and its pleasures. Health Risk Soc. **4**(2), 113–124 (2002)
74. Tick, A., Cranfield, D.J., Venter, I.M., Renaud, K.V., Blignaut, R.J.: Comparing three countries' higher education students' cyber related perceptions and behaviors during covid-19. Electronics **10**(22), 2865 (2021)
75. Griffiths, M.: Internet abuse and internet addiction in the workplace. J. Work. Learn. **22**(7), 463–472 (2010)
76. Anderson, N.E., Kiehl, K.A.: Psychopathy: developmental perspectives and their implications for treatment. Restor. Neurol. Neurosci. **32**(1), 103–117 (2014)
77. Anderson, N.E., Kiehl, K.A.: The psychopath magnetized: insights from brain imaging. Trends Cogn. Sci. **16**(1), 52–60 (2012)
78. Li, D., Zhang, W., Li, X., Zhen, S., Wang, Y.: Stressful life events and problematic internet use by adolescent females and males: a mediated moderation model. Comput. Hum. Behav. **26**(5), 1199–1207 (2010)
79. Dong, H., Yang, F., Lu, X., Hao, W.: Internet addiction and related psychological factors among children and adolescents in china during the coronavirus disease 2019 (covid-19) epidemic. Front. Psych. **11**, 751 (2020)
80. Deutrom, J., Katos, V., Al-Mourad, M.B., Ali, R.: The relationships between gender, life satisfaction, loneliness and problematic internet use during covid-19: Does the lockdown matter? Int. J. Environ. Res. Public Health **19**(3), 1325 (2022)
81. Zhou, Y., Li, D., Li, X., Wang, Y., Zhao, L.: Big five personality and adolescent internet addiction: the mediating role of coping style. Addict. Behav. **64**, 42–48 (2017)
82. Abd Rahim, N.H., Hamid, S., Kiah, M.L.M., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**(4), 606–622 (2015)
83. Zhang-Kennedy, L., Chiasson, S.: A systematic review of multimedia tools for cybersecurity awareness and education. ACM Comput. Surv. (CSUR) **54**(1), 1–39 (2021)
84. de Bruijn, H., Janssen, M.: Building cybersecurity awareness: the need for evidence-based framing strategies. Gov. Inf. Q. **34**(1), 1–7 (2017)