forensic sciences

MDPI

Article

Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking

Mary P. Aiken [1,*,†], Julia C. Davidson [1,†], Michel Walrave [2,†], Koen S. Ponnet [3,†], Kirsty Phillips [1] and Ruby R. Farr [1]

[1] Institute for Connected Communities, University of East London, Water Ln, London E15 4LZ, UK; j.davidson@uel.ac.uk (J.C.D.); infoicc@uel.ac.uk (K.P.); r.farr@uel.ac.uk (R.R.F.)
[2] Department of Communication Studies, University of Antwerp, 2000 Antwerp, Belgium; michel.walrave@uantwerpen.be
[3] Department of Communication Studies, Ghent University, 9000 Ghent, Belgium; koen.ponnet@ugent.be
* Correspondence: m.aiken@uel.ac.uk
† These authors contributed equally to this work.

Abstract: Adolescents are currently the most digitally connected generation in history. There is an ever-growing need to understand how typical adolescent risk-taking intersects with the vastly criminogenic potential of digital technology. Criminal hacking in older adolescents (16–19-year-olds) was assessed using an adapted Theory of Planned Behaviour (TPB) model, a cohesive theoretical framework that incorporates cognitive processes and human drivers (informed by psychology, cyberpsychology, and criminology theory). In 2021, a large-scale anonymous online survey was conducted across nine European countries. Criminal hacking was assessed using data from 3985 participants (M = 1895, 47.55%; F = 1968, 49.39%). This study formulated a powerful predictive model of youth hacking intention (accounting for 38.8% of the variance) and behaviour (accounting for 33.6% of the variance). A significant minority, approximately one in six (16.34%), were found to have engaged in hacking, and approximately 2% reported engaging in hacking often or very often. Increased age, being male, and offline deviant behaviour were significant predictors of hacking behaviour. In line with the TPB, intention was the strongest individual predictor of hacking behaviour, which in turn was significantly predicted by cognitive processes accounted for by TPB constructs: subjective norms of family and peers, attitudes towards hacking, and perceived behavioural control. These TPB constructs were found to be significantly associated with human factors of risk-taking, toxic online disinhibition, offline deviant behaviour, and demographic variables of age and gender. Implications for future research, interventions, policy, and practice are discussed.

Keywords: cybercrime; cyberdelinquency; cyberdeviance; hacking; adolescence; cyberpsychology; theory of planned behaviour

Citation: Aiken, M.P.; Davidson, J.C.; Walrave, M.; Ponnet, K.S.; Phillips, K.; Farr, R.R. Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. *Forensic Sci.* **2024**, *4*, 24–41. https://doi.org/10.3390/forensicsci4010003

Academic Editor: Nicholas Kolokotronis

Received: 18 December 2023
Revised: 23 January 2024
Accepted: 25 January 2024
Published: 30 January 2024

1. Introduction

Adolescence is a key psychosocial developmental phase, specifically regarding the development of identity, autonomy, intimacy, and also personal achievements. Three key indicators are universally observed in adolescence, pointing to an underlying biological mechanism, namely increased risk-taking, increased novelty-seeking, and increased peer association and affiliation [1]. These indicators of adolescent risk-taking are well established; however, it is less well understood how these behaviours manifest in the digital space. Adolescents are currently the most digitally connected generation in history [2], reporting to spend over half of their waking hours (8.39 h) on their digital devices [3]. Recent surveys have found that cyberdeviance and cybercrime are almost ubiquitous in the teen population. Recent large-scale research has identified that approximately two-thirds of the youth population self-report to engage in some form of cybercriminal or cyberdeviant behaviour, inclusive of hacking [4]. Notably, rates increase with age. In a study conducted

in Australia, rates of cyber risk-taking were high and increased over a three-year period from 79.6% in 2018 to 89.5% in 2021 within the same cohort of teens [5]. It is imperative to not only understand the factors associated with cyberdeviance, but to design interventions to prevent harm arising from these behaviours in cyber contexts.

The term 'deviance' refers to the violation of established norms and approved rules, encompassing serious behaviours, including crimes and delinquent acts (crimes conducted by juveniles), and behaviours that are not always punishable by law, but that are either antisocial or harmful to the individual or others [6,7]. The term 'cyberdeviance' refers to the intersection of these behaviours and digital technology and is inclusive of a wide range of behaviours that not only violate societal norms but also violate legally proscribed rules [8]. To what extent harmful online behaviours are considered a crime and how to conceptualise 'cybercrime' continues to be vigorously debated; however, the general consensus to date is that both terms (cybercrime and cyberdeviance) are considered to refer to what could be described as a broad spectrum of criminal and harmful cyber behaviours, a supposition now supported by recent empirical research [4]. Importantly in the context of this study, a recent large-scale self-report survey found that approximately half (47.76%) of the sample (n = 7974) reported engaging in some form of cybercrime, and when taking into account cyberdeviant and potentially risky online behaviours, this number increased to just over two-thirds (69.1%) [4].

Both terms include behaviours unique to the cyber landscape, the transition of pre-existing criminal behaviours occurring with the use of, or facilitated by, technology, as well as the new evolution of crime behaviours due to advancements in technology (for a discussion of definitional issues, see Phillips et al., 2022 [9]). Furthermore, these terms are used interchangeably to refer to the same spectrum of behaviours precisely to circumnavigate problems that arise from, for example, differences in cybercrime legislation across jurisdictions [9].

A particular cybercriminal behaviour relevant to researchers, policymakers, and law enforcement is that of criminal 'hacking.' This behaviour is entirely exclusive to the cyber landscape (i.e., it cannot occur offline or in the so-called real world), termed 'cyber-dependent' [10], and is therefore unique compared to other forms of cybercrime and cyberdeviance. Whilst there is no offense of 'hacking', the term refers to a constellation of behaviours that affect the confidentiality, integrity, and availability of computer data and systems [11]. Furthermore, legal systems define hacking (access, interception, interference, and misuse of computer data and systems) as an illegal act, irrelevant of motive, intent, or purpose [12]. Hacking among youth populations is known to be prevalent, although exact estimates of perpetration rates vary across studies (dependent on the operationalisation of the term 'hacking,' research methodology, and sampling methodology), estimates range from approximately one in eleven [13], in a large-scale academic study, to one in four [14] (p. 692), in a small industry study.

2. Understanding the Phenomenology of Hacking and Profile of Hackers

Foundational work concerning cybercriminality has identified a number of pertinent factors that may inform youth pathways into cybercrime, such as age, gender, computer literacy, interest in and aptitude for technology, willingness to engage in low-level illegal Internet-related activity, deriving intrinsic pleasure from increased challenges, and the need for affiliation, affirmation, and online peer networks that normalise and encourage illegal behaviour [15,16]. Holt and Bossler (2015) [17] note that research regarding hacking has increased over the last two decades, specifically regarding insights into key predictors of hacking among adolescent and adult samples. Further, Back et al., 2018 [18], highlight that there is a large number of studies exploring hacker culture, characteristics, perceptions, types, and techniques [19–26].

Work concerning cybercrime perpetration is primarily descriptive and there exist proportionally few empirical research studies that are underpinned by established academic theory (see Bossler, 2019 [27], for an overview of the application of criminology theory to

cybercrime). A promising model to explore cognitive processes explaining cybercriminal and cyberdeviant behaviours is that of Ajzen's (1985) [28] Theory of Planned Behaviour (TPB), and whilst some exploratory work has considered the relationship between the Theory of Reasoned Action (TRA) [29] and hacking behaviour [30], no study to date has applied TPB to adolescent criminal hacking. Furthermore, there is a paucity of studies exploring the 'human element' of hacking, particularly in youth populations, and factoring in cognitive processes that may underly cybercriminal intention. It is recognised in the literature that one of the most intractable threats to cybersecurity is the sociotechnical element, meaning the behaviour of those behind the technology. The 'human factor' has been recognised as being 'the weakest and most obscure link in creating safe and secure digital environments' [31] (p. 338). Rather, for these forms of crimes, there is a focus on understanding their technical drivers and creating technical interventions (cybersecurity or infosec interventions); therefore, it is necessary to factor the human, and specifically youth, perpetrators into the cybercrime equation. The TPB bridges a gap in the literature by offering a cohesive theoretical framework for understanding cognitive processes and key human factors regarding hacking, with a corresponding analytical framework to determine the predictive power of these individual variables and how they interact.

3. Application of Academic Theory

Ajzen's 1985 [28] Theory of Planned Behaviour (TPB) is a cognitive theory that proposes that an individual's decision to engage in a specific behaviour, such as illegal hacking or cyberfraud, can be predicated by their intention to engage in that behaviour. Notably, 'intentions are assumed to capture the motivational factors that influence a behaviour; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behaviour. As a general rule, the stronger the intention to engage in a behaviour, the more likely should be its performance [32]' (p. 181). TPB has already been applied in research concerning risky online behaviours of adolescents, such as cyberbullying [33] and sexting [34]. Owen, 2016 [30], has highlighted the theoretical potential utility of The Theory of Reasoned Action [29], in terms of intention, and the Theory of Planned Behaviour [32], in terms of 'the hacker's appraisal of whether the hacking is within their locus of control directly influences their hacking intentions and the subsequent hacking behaviour, termed as perceived behavioural control' [35] (p. 2), to understanding why individuals chose to engage in hacking behaviours. Moreover, the TPB also incorporates aspects of social influence, which is particularly salient during the period of adolescent development [1].

4. Research Aim

Given the above-identified potential risks of youth hacking and that engaging in these behaviours may set young people onto a trajectory of cyberdelinquency and criminality that can have life-altering consequences [15], it is vital to comprehensively understand the human factors that lead young people on these pathways in order to inform intervention mechanisms for policymakers and educators. The application of the TPB to youth hacking, in particular, provides a unique conceptual framework that can be adapted to incorporate both cognitive processes (TPB constructs of attitudes, subjective norms, perceived behavioural control, intentions) as well as key identified human factors (risk-seeking, toxic online disinhibition, and offline deviant behaviours, explained in greater detail under hypothesis development). The current study was conducted with older adolescents (ages 16–19), as these ages represent a transition from being a juvenile to legal adulthood and, therefore, to being held responsible for any illegal action taken. As such, the findings of our study may prove key to creating interventions and diversion from justice programmes.

5. Hypothesis Development

According to the TPB, intention is believed to directly account for the manifestation of the behaviour of interest, if that behaviour is under volitional control, which, in turn,

is affected by attitudes towards the behaviour ('favourable or unfavourable evaluation or appraisal of the behaviour in question'), subjective norms (SNs, 'the perceived social pressure to perform or not to perform the behaviour'), and perceived behavioural control (PBC, 'the perceived ease or difficulty of performing the behaviour'). Additionally, the TPB predicts that perceived behavioural control directly predicts the behaviour [32] (p. 188).

Therefore, this study seeks to investigate the cognitive processes that underlie youth hacking by determining the factors that lead to intention (attitudes, SNs, and PBC), which can then lead to the behaviour. Additionally, this model will be complemented with demographic variables (i.e., age and gender), as well as psychological and criminological factors (i.e., risk-seeking, toxic online disinhibition, and offline deviant behaviours). There exist studies and literature linking these demographic and human driver variables as important predictors of deviancy, criminality, cyberdeviancy, and cybercriminality—youth hacking in particular—that are further discussed in later sections. Given the novelty of this approach, there is a lack of literature linking these variables to TPB constructs specifically; therefore, these variables will be incorporated within the proposed adapted TPB model to assess their association with TPB constructs.

5.1. Hacking Behaviour

Academic studies investigating hacking perpetration within youth age groups, defining hacking in a similar way, determined that the perpetration rate of hacking behaviour was 9.3% [13]. However, there is some evidence that hacking rates have increased in the youth population during and following COVID-19 pandemic [36]. For example, in the UK, the NCA, 2022 [37], reported that cyberattacks on school networks and websites by young people had, in fact, doubled during the pandemic. Therefore, arguably, it can be predicted that perpetration rates may also have increased since 2018.

5.2. Behavioural Intention

It has been suggested that intention to engage in a behaviour is the strongest predictor of exhibiting that behaviour, with the exception of when that behaviour is outside of one's behavioural control [32]. Whilst there are some environmental constraints (e.g., availability of resources) and personal constraints (e.g., ability), which are accounted for by PBC measures, hacking is mainly considered a behaviour that is dictated by volitional control [32,38], similar to cyberbullying [33]. We therefore propose the following hypothesis:

Hypothesis 1 (H1): *Intention to engage in hacking will be positively associated with hacking behaviour.*

5.3. Attitudes

Criminological theory, namely drift, prescribes that 'techniques of neutralisation' will be employed when committing deviant behaviours, predicting that individuals will attempt to justify or neutralise wrongdoing through normalising of behaviours, denial of harm, or even placing onus on victims [39,40]. Many hackers may not necessarily perceive hacking as illegal or wrong; this perception is arguably compounded by pro-social or activist portrayals of hackers within the media [41,42]. Furthermore, the pervading narratives about hacking behaviour within hacker subculture strongly influence attitudes within this group, first outlined in the 'The Hacker Manifesto' [43]. Those within the hacking community often hold positive attitudes towards hacking and hacking behaviours; a key ethos of the so-called 'hacker ethic' centres on free access to information and technology [41]. Further, the meritocracy within hacker subculture can supersede the perception of morality or legality, meaning the only aspect of the behaviour that truly matters is the skill needed to complete the hack [41]. We therefore propose the following hypothesis:

Hypothesis 2 (H2): *The more permissive young people's attitudes towards hacking, the higher their intention to engage in hacking.*

5.4. Subjective Norms

Adolescence is considered a salient period of identity formation, where family and peers have a formative influence [44,45]. One of the triad of behaviours universally observed in adolescence is the social shift towards more peer-based affiliations and interactions [1,46]. Criminological research has demonstrated that exposure to and association with deviant peers is generally one of the strongest predictors of delinquency and criminality [41,47], as well as hacking, specifically [41,48–50]. We therefore propose the following hypothesis:

Hypothesis 3 (H3): *There will be a positive relationship between subjective norms and hacking intentions, meaning perceived permissive attitudes held by parents (H3a) and peers (H3b) are positively related to adolescents' hacking intentions.*

5.5. Perceived Behavioural Control

PBC encompasses two constructs: one represents an internal belief, meaning the individual's own internal perception of their ability to carry out the behaviour, and the second represents the actual availability of resources to engage in a behaviour [32]. Within this study, PBC items focus on intrinsic beliefs only, measuring the internal perception of skill, ability, and confidence to carry out hacking behaviours. There are arguably advanced skills or knowledge that need to be acquired to perform even minor hacking behaviours or access hacking forums, e.g., use of the Onion router (TOR) and programming skills. Furthermore, hackers pride themselves on their abilities and skills; a key characteristic of hackers is the desire for technological mastery [41]. Therefore, arguably only those who engage in hacking, or intend to, could reasonably be expected to seek to increase their own skills and abilities and correspondingly exhibit a higher PBC. We therefore propose the following hypothesis:

Hypothesis 4 (H4): *There will be a positive relationship between PBC and hacking intention (H4a) and PBC and hacking behaviour (H4b).*

5.6. Demographic Variable: Age

Academic research has identified that hacking behaviour tends to begin in adolescence and those heavily involved are typically young. This is in line with other types of offending according to the typical age–crime curve relationship between offending and age [19,21,41,51,52]. The UK's National Crime Agency's (NCA) National Cyber Crime Unit (NCCU) has recently shared that many of the referrals regarding cybercrime are for children of secondary school age, as young as nine, but with a median age of 15 [37].

Additionally, longitudinal research conducted by Logos et al., 2021 [5], found that rates of any form of cyber risk-taking were high and increased over a three-year period from 79.6% in 2018 (13–14-year-olds) to 89.5% in 2021 (same cohort at 15–16 years old). Research has theorised that many young hackers often naturally desist by their mid-20s, which is again in line with youth offending in other areas [25,53,54]; however, as this is beyond the age group within this study, it is predicted that age will be related to increased hacking perpetration. We therefore propose the following hypothesis:

Hypothesis 5 (H5): *Increasing age will be associated with greater levels of hacking behaviour.*

5.7. Demographic Variable: Gender

Qualitative research has observed that there is a gender gap in relation to hacking [21,41,54,55], and males are also more likely to self-report involvement in different types of hacking [41,48,50,56]. There are longstanding speculative reasons for the gender gap, one being that it is reflective of the general gendering of technology use [54,57] and the other being that females are much less likely to engage in crime and delinquency, which

is a well-established finding in traditional real-world crime [58]. We therefore propose the following hypothesis:

Hypothesis 6 (H6): *Males will exhibit greater levels of hacking behaviour.*

5.8. Human Factor: Risk-Seeking

Low self-control or impulsivity has been found to be a key personality trait associated with criminal behaviours. Gottfredson and Hirschi's 1990 [59] general theory of crime proposes that low self-control interacts with opportunity to constitute a major cause of criminal behaviour. Low self-control has been found to increase the likelihood of involvement in hacking in both college populations [48–50] and adolescent populations [18,41,56,60,61]. A component of low self-control salient in adolescent years is that of risk-taking [1,46]. Grasmick et al., 1993 [62], developed a scale to measure Gottfredson and Hirschi's, 1990 [59], theoretical conceptualisation of low self-control, including a subscale to measure risk-seeking, which is used in the present study. We therefore propose the following hypothesis:

Hypothesis 7 (H7): *Greater levels of risk-seeking will be associated with greater levels of hacking behaviour (H7a). In addition, risk-seeking will be assessed for association with other TPB constructs; greater levels of risk-seeking will be associated with more positive attitudes towards hacking (H7b), more favourable subjective norms of parents (H7c) and friends (H7d), higher PBC to engage in hacking (H7e), and higher intention (H7f).*

5.9. Human Factor: Toxic Online Disinhibition

The 'online disinhibition effect', first proposed by Suler (2004) [63], is used to describe the phenomenon whereby people may feel more liberated and able to express themselves when online. Suler (2004) [63] further differentiates between toxic and benign disinhibition. Benign disinhibition may be when individuals online overshare or become unusually kind or generous, whereas with toxic disinhibition, individuals become unusually unkind online (displaying rudeness, hate, making threats, etc.) or explore the deviant or criminal environments that can be found online, particularly on the Dark Web [63,64].

Udris (2017) [65] used structural equation modelling to explore predictors of both offline and online deviance, and determined that toxic disinhibition was the strongest predictor of online deviance, whereas benign disinhibition was found to be unrelated to deviant behaviour. Therefore, the present study focuses on the relationship between toxic disinhibition and TPB constructs. We therefore propose the following hypothesis:

Hypothesis 8 (H8): *Greater levels of toxic online disinhibition will be associated with greater levels of hacking behaviour (H8a). In addition, toxic online disinhibition will be assessed for association with other TPB constructs: greater levels of toxic online disinhibition will be associated with more positive attitudes towards hacking (H8b), more favourable subjective norms of parents (H8c) and friends (H8d), higher PBC to engage in hacking (H8e), and higher intention (H8f).*

5.10. Human Factor: Offline Deviant Behaviour

Foundational criminology theory, namely 'drift' [40], posits that delinquent values are held by the majority, but these values are suppressed through learned skills and adherence to subjective norms. While there is a higher tendency for delinquency when young, some 'drift' between conformity and deviance throughout their lives, using 'techniques of neutralisation' to justify their behaviour, e.g., denial of responsibility [40]. The concept of 'drift' has been explored in digital contexts to explore cyberdelinquency [13,39,66]. A key indication of 'drift' is the propensity to engage in different forms of delinquency, as indicated by engaging in both offline and online deviant behaviours. Brewer et al. (2018) [13] found moderate to strong correlations between online and offline delinquency, and risk-taking was equally correlated to both offline and online delinquency. Self-report surveys have found a significant overlap between online and offline delinquency. Those who engage in

risky behaviours offline are 6.8 to 13 times more likely to have engaged in cyber risk-taking ([5,67]). Furthermore, these studies determined that physical risk-taking (offline delinquent behaviours) was a strong predictor of online delinquency [5,67]. We therefore propose the following hypothesis:

Hypothesis 9 (H9): *Greater levels of offline deviant behaviour will predict greater levels of hacking behaviour (H9a). In addition, offline deviant behaviour will be assessed for association with other TPB constructs: greater levels of offline deviant behaviour will be associated with more positive attitudes towards hacking (H9b), more favourable subjective norms of parents (H9c) and friends (H9d), higher PBC to engage in hacking (H9e), and higher intention (H9f).*

6. Method

6.1. Participants

An online survey questionnaire was completed by 7974 participants aged 16–19 across nine European countries, representing a geographic spread of Europe. A quota sampling approach was used, and participants were recruited from existing panels via a research agency. The sample was recruited according to country or region with 1000 (12.5%) recruits in each of the seven countries and one region: namely the UK, France, Spain, Germany, Italy, the Netherlands, Romania, and the region of Scandinavia (comprised of 70% of participants from Sweden and 30% from Norway). Due to the smaller panel sizes in Sweden and Norway, both samples were combined to form a 'region'. Within each country, the sample was recruited to have an even split of the age range (25% 16-, 17-, 18-, and 19-year-olds) and even split of gender (50% male and female; participants with other gender identities were also recruited).

This study was conducted as part of the wider CC-DRIVER ('Understanding the drivers of cybercriminality, and new methods to prevent, investigate, and mitigate cybercriminal behaviour') research initiative and the H2020 research programme. The sample was divided within this study. For reasons of survey length, the questions related to hacking were presented and completed by 3985 (49.97% of the final sample) participants. The current analyses are based on this subsample. Descriptive characteristics of the sample are provided in Table 1.

Table 1. Descriptive characteristics (gender and country).

	Male		Female		Identify in Another Way		Prefer Not to Say		Total
	n	%	*n*	%	*n*	%	*n*	%	
UK	237	48.67	232	47.64	16	3.29	2	0.41	487
Spain	244	47.84	253	49.61	10	1.96	3	0.59	510
France	243	45.94	267	50.47	12	2.27	7	1.32	529
Germany	251	50.20	237	47.40	10	2.00	2	0.40	500
Italy	237	48.97	224	46.28	20	4.13	3	0.62	484
Netherlands	201	43.04	252	53.96	9	1.93	5	1.07	467
Romania	243	48.50	249	49.70	6	1.20	3	0.60	501
Sweden	177	48.10	180	48.91	7	1.90	4	1.09	368
Norway	62	44.60	74	53.24	2	1.44	1	0.72	139
Total	1895	47.55	1968	49.39	92	2.31	30	0.75	3985

This study was conducted in accordance with the ethical standards of the British Psychological Association (BPS), with approval from (blinded for the review), as well as an independent CC-DRIVER Ethics Board. Data were collected with the strictest privacy and legal regulations and in adherence with data protection regulations (GDPR).

6.2. Procedure

Data collection took place over approximately three months (June–August 2021); the average time to complete was 32.29 min. All questions were in multiple-choice and

forced-choice response format. The survey was uploaded to an online survey platform using Ex-plor Strat7 (a GDRP-compliant ResearchBods, Leeds, UK) proprietary-owned Communities platform). Before being able to access the survey, participants had to give informed consent, had to pass captcha, confirm they were between 16–19 years old, and accept cookies (to prevent multiple responses from one user). Participants were free to withdraw, by exiting, at any point in the survey. Only complete surveys were taken forward to analysis. Once completed, participants were debriefed and provided with support links.

6.3. Measures

The phenomenon of hacking was introduced as follows: 'On the Internet, some people engage in hacking. By hacking, we mean the unauthorised access and use of computer systems. This ranges from hacking into a system, to stealing personal information, to hacking someone's social media accounts.' The operationalisation of hacking was informed by legal statutes [11], academic literature [56,68], and an internal survey piloting process with the target age group. The measures were created following the recommendations of Ajzen, 2011 [69]. All items and mean scores of the items are presented in Table 2.

Table 2. Item content and descriptive statistics.

	Min	Max	Mean	SD
Behaviour				
I have engaged in hacking.	0	4	0.25	0.66
Intention				
I intend to engage in hacking.	1	7	1.5	1.17
I expect to hack someone's computer.	1	7	1.46	1.09
I plan to hack a computer.	1	7	1.43	1.08
Attitudes				
Legal—Illegal	1	7	6.14	1.61
Right—Wrong	1	7	5.95	1.66
Normal—Not normal	1	7	5.63	1.76
Not serious—Serious	1	7	5.98	1.58
Not harmful—Harmful	1	7	5.97	1.59
Not risky—Risky	1	7	6.07	1.56
Subjective Norm Parents				
My parent(s)/guardians would not have a problem with me hacking someone's computer.	1	7	1.71	1.52
My parent(s)/guardians would approve of me hacking someone's computer.	1	7	1.54	1.23
Subjective Norm Friends				
My friends would not have a problem if I engage in computer hacking.	1	7	2.18	1.75
My friends would approve of me hacking someone's computer.	1	7	2.00	1.59
Perceived Behavioural Control				
I have the skills to hack a computer.	1	7	1.73	1.38
It is easy for me to hack a computer.	1	7	1.62	1.26
I am able to hack a computer.	1	7	1.78	1.46
Online (Toxic) Disinhibition				
I don't mind writing insulting things about others online, because it's anonymous.	0	3	0.41	0.78
It is easy to write insulting things online because there are no repercussions.	0	3	1.02	1.09
There are no rules online therefore you can do whatever you want.	0	3	0.61	0.88
Writing insulting things online is not bullying.	0	3	0.46	0.84
Offline Deviant Behaviour				
Used cocaine or heroin?	0	4	0.2	0.65
Sold drugs (e.g., hash, weed, cocaine, ecstasy, amphetamines, etc.)?	0	4	0.21	0.68
Drawn graffiti on buildings or other locations (e.g., school, public transports, walls, etc.)?	0	4	0.27	0.73
Used a motorbike or a car to go for a ride without the owner's permission?	0	4	0.21	0.67
Used LSD ("acid"), ecstasy ("tablets"), or amphetamines ("speed")?	0	4	0.23	0.7
Stolen something worth more than 50 euros (e.g., in shops, at school, from someone, etc.)?	0	4	0.23	0.7
Hit an adult (e.g., teacher, family, security guard, etc.)?	0	4	0.26	0.72
Broken into a car, a house, shop, school, or other building?	0	4	0.24	0.7

Table 2. *Cont.*

	Min	Max	Mean	SD
Damaged or destroyed public or private property (e.g., parking meters, traffic signs, product distribution machines, cars, etc.)?	0	4	0.25	0.69
Carried a weapon (e.g., knife, pistol, etc.)?	0	4	0.27	0.75
Risk-seeking				
I like to test myself every now and then by doing something a little risky.	1	4	2.04	0.97
Sometimes I will take a risk just for the fun of it.	1	4	2.02	0.99
Excitement and adventure are more important to me than security.	1	4	1.94	0.93

6.4. Hacking Behaviour

Hacking behaviour was measured with a single item ('I have engaged in hacking.'). Respondents could answer the question with 1 = never, 2 = rarely, 3 = sometimes, 4 = often, or 5 = very often.

6.5. Behavioural Intention

Three items measured intention to engage in hacking. The items were scored along a 7-point Likert scale ranging from 1 = totally disagree to 7 = totally agree. The internal consistency of the items was good ($\alpha = 0.94$).

6.6. Attitudes

Respondents rated their attitude by means of six semantic differential 7-point scales, ranging from 1 to 7, shown in Table 2. Items were presented from positive to negative; therefore, higher scores indicate less positive attitudes. The reliability of the scale was good ($\alpha = 0.93$).

6.7. Subjective Norm

The subjective norms of friends and parents was measured with two items each. The four items were assessed using a 7-point Likert scale, with item responses ranging from 1 = totally disagree to 7 = totally agree, including a null item (0 = 'Does not apply to me.'). All scales were reliable, with $\alpha = 0.90$ for friends and $\alpha = 0.78$ for parents.

6.8. Perceived Behavioural Control

Three items measured participants' confidence that they are capable of performing the behaviour. All items were scored on a 7-point Likert scale, ranging from 1 = totally disagree to 7 = totally agree. The Cronbach's alpha of the scale was 0.91.

6.9. Toxic Online Disinhibition

Online disinhibition was measured with four items from the toxic disinhibition factor of Udris' online disinhibition scale (2014) [70]. All items were scored on a 4-point Likert scale, ranging from 0 = disagree to 4 = agree. The Cronbach's alpha of the scale was 0.72.

6.10. Offline Deviant Behaviour

A subset of 10 items of the Deviant Behaviour Variety Scale (DBVS) [71] was adopted to measure offline deviant behaviour. All items were scored on a 4-point Likert scale, ranging from 0 = never to 4 = very often. The Cronbach's alpha of the scale was 0.96.

6.11. Risk-seeking

To measure risk-seeking, three items were used from a subscale of Grasmick et al.'s, 1993 [62], low self-control scale. All items were scored on a 4-point Likert scale, ranging from 1 = fully disagree to 4 = fully agree. The Cronbach's alpha of the scale was 0.80.

6.12. Data Analysis

To investigate the relationships among the TPB constructs, structural equation modelling was applied to the collected data using Mplus 8.7 [72]. The analyses were carried out in the following way. Firstly, a measurement model was built and the authors examined whether the observed variables reliably reflected the hypothesised latent variables in the research model. Secondly, the authors estimated a structural model with attitude, subjective norms of parents and friends, perceived behavioural control, online toxic disinhibition, risk-seeking, and offline deviant behaviour as predictor variables and with behavioural intention and self-reported hacking behaviour as endogenous variables. Age and gender were included as covariates in the model. Given the low percentages of people who identified themselves in another way (2.31%) and those who declined to answer (0.75%), only male and female respondents were included in the analyses. Structural equation modelling results were obtained with maximum likelihood mean adjusted, because preliminary tests suggested that self-reported behaviour was a not normally distributed dependent variable.

The model fits of the measurement and path models were evaluated according to several fit indices. Given that the chi square is almost always significant and not an adequate test of the model fit [73,74], the authors also reported the Comparative Fit Index (CFI) [75], the Tucker–Lewis index (TLI) [76], the Root Mean Square Error of Approximation (RMSEA) [77], and the Standardised Root Mean Square Residual (SRMR) [74]. The CFI and TLI range from 0 to 1.00, with a cut-off of 0.95 or higher indicating that the model provides a good fit and 0.90 indicating that the model provides an adequate fit [78,79]. RMSEA values below 0.05 indicate a good model fit, and values between 0.06 and 0.08 indicate an adequate fit [80]. The SRMR is a standardised summary of the average covariance residuals [74]. A relatively good model fit is indicated when the SRMR is smaller than 0.08 [79].

7. Results

7.1. Descriptive Findings

In total, 16.34% (n = 651) of the participants had engaged in the behaviour; one out of ten (9.91%, n = 395) indicated they had rarely engaged in hacking, 4.42% (n = 176) engaged in it sometimes, 1.46% (n = 58) did so often, and 0.55% (n = 22) did so very often. Table 3 displays the correlations between the research constructs used in the model. All constructs were significantly related to each other, with $p < 0.001$.

Table 3. Correlations among the constructs.

		1	2	3	4	5	6	7	8
1	Attitudes								
2	SN Parents	−0.408							
3	SN Friends	−0.378	0.761						
4	PBC	−0.274	0.472	0.484					
5	Intention	−0.385	0.584	0.529	0.441				
6	Behaviour	−0.400	0.424	0.365	0.382	0.544			
7	Offline Deviant Behaviour	−0.262	0.357	0.247	0.307	0.295	0.348		
8	Online Toxic Disinhibition	−0.243	0.348	0.369	0.327	0.284	0.263	0.458	
9	Risk-Seeking	−0.086	0.194	0.257	0.240	0.166	0.148	0.262	0.369

7.2. Fit of Measurement Model

The measurement model provided a good fit for the data; chi square (492) = 1368.25, $p < 0.001$; CFI = 0.98, TLI = 0.98, RMSEA = 0.022 (CI: 0.020–0.0023), and SRMR = 0.027. All variables were treated as latent constructs, with the exception of the single-item measure for behaviour. All factor loadings were significant and above 0.48. Gender and age were subsequently included as covariates in the analysis and examined for the relationships between age, gender, and the study variables. The structural model (presented in Figure 1) was adjusted for the influence of these variables.

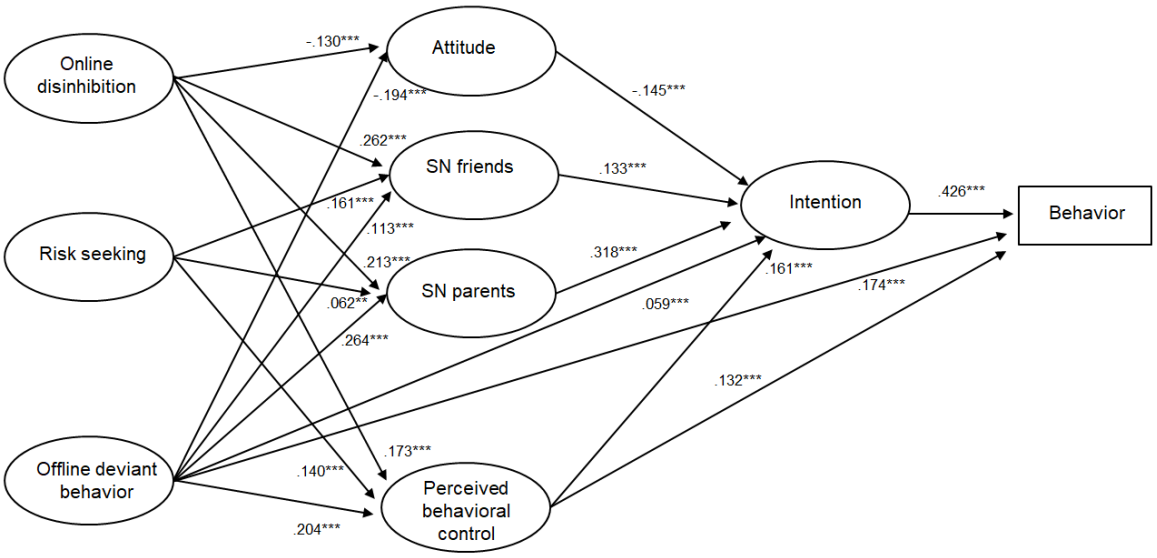

Figure 1. An adapted TPB Model of Criminal Hacking. Note: all reported coefficients outside brackets are standardised values, adjusted for the influence of gender and age. Non-significant paths are not shown. ** $p < 0.01$; *** $p < 0.001$.

The results of the fit statistics of the subsequent model indicate an adequate model fit: chi square (548) = 3740.55, $p < 0.001$, CFI = 0.96, TLI = 0.96, RMSEA = 0.040 (C.I. 90%: 0.039–0.041), SRMR = 0.080. The authors' analyses reveal that attitude, subjective norms (friends and parents), perceived behavioural control, disinhibition, offline deviant behaviour, and risk-seeking, together with the covariates gender and age, account for 38.8% of the variance in hacking intention, and when combined with intention, explain 33.6% of the variance in young people's engagement in hacking. The results of the structural model are presented in Figure 1.

7.3. Fit of Structural Model: TPB Constructs

The most important predictor of hacking behaviour is intention ($\beta = 0.426$, $p < 0.001$), supporting H1, and perceived behavioural control ($\beta = 0.132$, $p < 0.001$) also made a significant contribution, supporting H4b.

Intention to hack was mostly influenced by the subjective norms of parents and friends ($\beta = 0.318$, $p < 0.001$ and $\beta = 0.133$, $p < 0.001$, respectively), supporting both H3a and H3b, along with attitudes ($\beta = -0.145$, $p < 0.001$), supporting H2, and perceived behavioural control ($\beta = 0.161$, $p < 0.001$), supporting H4a.

7.4. Fit of Structural Model: Human Factors

Contrary to expectations, risk-seeking was not significantly related to hacking behaviour ($\beta = -0.007$, $p = 0.688$), rejecting H7a, hacking intention ($\beta = 0.000$, $p = 0.990$), rejecting H7f, or attitudes ($\beta = -0.001$, $p = 0.946$), rejecting H7b. However, risk-seeking was significantly associated with subjective norms of parents ($\beta = 0.062$, $p < 0.001$), supporting H7c, and friends ($\beta = 0.161$, $p < 0.001$), supporting H7d, and perceived behavioural control ($\beta = 0.140$, $p < 0.001$), supporting H7e.

Contrary to the authors' expectations, toxic online disinhibition was not significantly related to hacking behaviour ($\beta = 0.024$, $p = 0.200$), rejecting H8a, or hacking intention ($\beta = 0.012$, $p = 0.539$), also rejecting H8f. However, toxic disinhibition was significantly associated with attitudes ($\beta = -0.130$, $p < 0.001$), supporting H8b, subjective norms of parents ($\beta = 0.213$, $p < 0.001$), supporting H8c, and friends ($\beta = 0.262$, $p < 0.001$), supporting H8d, and perceived behavioural control ($\beta = 0.173$, $p < 0.001$), supporting H8e.

Offline deviant behaviour strongly influenced both hacking behaviour ($\beta = 0.174$, $p < 0.001$), supporting H9a, and hacking intentions ($\beta = 0.059$, $p < 0.001$), supporting H9f. It

was further found that offline deviant behaviour was significantly associated with attitudes ($\beta = -0.194$, $p < 0.001$), supporting H9b, subjective norms of parents ($\beta = 0.264$, $p < 0.001$), supporting H9c, and friends ($\beta = 0.113$, $p < 0.001$), supporting H9d, and with perceived behavioural control ($\beta = 0.204$, $p < 0.001$), supporting H9e.

7.5. Effect of Age and Gender on Model Constructs

Age was found to be significantly associated with hacking behaviour ($\beta = 0.07$, $p < 0.001$), supporting H5. In addition, age was found to be significantly associated with the subjective norms of parents ($\beta = 0.05$, $p < 0.004$) and offline deviant behaviour ($\beta = 0.06$, $p < 0.001$). Age was not found to be significantly associated with other model constructs.

Males were found to have greater levels of hacking behaviour ($\beta = -0.15$, $p < 0.001$), supporting H6. In addition, gender was found to be significantly associated with all but one of the model constructs, namely risk-seeking. Males were more likely to have greater intentions to hack ($\beta = -0.15$, $p < 0.001$), more positive attitudes towards hacking ($\beta = 0.19$, $p < 0.001$), more favourable subjective norms of parents ($\beta = -0.15$, $p < 0.001$) and friends ($\beta = -0.18$, $p < 0.001$), greater perceived behavioural control ($\beta = -0.21$, $p < 0.001$), greater levels of toxic online disinhibition ($\beta = -0.22$, $p < 0.001$), and greater levels of offline deviant behaviour ($\beta = -0.14$, $p < 0.001$).

8. Discussion

8.1. Result Summary

Approximately one in six participants (16.34%) reported to have engaged in hacking. Compared to previous research [13], this study found a higher percentage of young people engaging in hacking. This could be due to methodological differences, in-person versus anonymous online survey data collection, or the finding that cybercrime is rapidly increasing, accelerated by the COVID-19 pandemic [36], and the fact that children of an increasingly young age are reportedly becoming involved in hacking [37].

In line with the TPB, intention was the strongest predictor of hacking behaviour, and PBC also had a significant influence on behaviour [32,38]. This study, in line with other research, also identified that older adolescents (age) [5,19,21,41,51,52,81], males (gender) [21,41,48,50,54–56,81], and higher incidence of offline deviant behaviour were also significantly associated with increased perpetration of hacking behaviour [5,13,67]. Also, in line with the TPB [32], intention was significantly and most strongly predicted by TPB constructs, SNs of family and peers, attitudes, and PBC, in the hypothesised direction. Moreover, a higher incidence of offline delinquent behaviour and gender were also found to be significant predictors of intention; a higher incidence of offline delinquency predicted greater intention to hack, and males were more likely to have intentions to engage in hacking.

More positive attitudes towards hacking were significantly associated with higher levels of toxic online disinhibition, more offline deviant behaviour, and being male. This indicates that those who are more inclined to engage in risky and harmful behaviours may be engaging in 'techniques of neutralisation', as predicted by drift theory [39], and the general increased transgressive potential associated with male adolescents [82]. More permissive attitudes from friends and family were significantly associated with increased risk-seeking, higher levels of toxic online disinhibition, more offline deviant behaviour, and being male. This is in line with wider literature that examines deviance in adolescence, e.g., alcohol misuse at young age, and that found liberal attitudes linked to increased deviant behaviours, increased family conflict, and lower levels of parental monitoring [83].

Greater perceived behavioural control, operationalised as perceived technical ability to commit a hack in this study, is significantly associated with increased risk-seeking, higher levels of toxic online disinhibition, more offline deviant behaviour, and being male. This indicates, as hypothesised, those wanting to engage in hacking (driven by a general propensity for risk-taking) may seek to increase their technical skills.

In addition, as adolescents age, they are significantly more inclined to engage in offline deviant behaviour. This is in line with other research [5] and, in general, the age–crime curve relationship between offending and age [19,21,51,52,81]. Further, males were more likely to have higher levels of toxic online disinhibition. This is in line with other studies investigating online hate [84] and cyberbullying [70]. Males are also more likely to engage in more offline deviant behaviour, which is again in line with previous research. One of the most consistent findings in criminology is that males are much more likely to commit offline crime and delinquency than females [58].

8.2. Limitations and Future Research

Notwithstanding this study's findings, the results should be considered in light of this study's limitations. First, as the survey used a cross-sectional design, future research could consider a longitudinal study to examine how behaviours and associated factors change over time. This would corroborate this study's cross-sectional findings about associated factors and add further understanding about changing motivations and how online risky behaviours escalate to criminal acts.

Second, this survey was a self-report measure, which can elicit answers that are influenced by social desirability; however, this was somewhat mitigated by the use of an anonymous online survey design. Future studies may consider a measure of social desirability as a moderating factor.

Third, hackers are not one homogenous group; hackers differ according to the legality of their activity (i.e., illegal 'black hat' hackers and ethical 'white hat' hackers), their skill level, and their ideology [68]. Given the heterogeneity in the hacker population, further work is needed to systematically explore what human factors apply to large groups (e.g., across multiple different hacker types), specific subtypes, or even small groups of individuals (e.g., high-profile female criminal hackers). Further TPB models that differentiate between different hacking behaviours or alternative methods, such as latent variable analysis or factor analysis, could help differentiate between the profiles of these different groups.

Fourth, the present study focussed on older adolescents (16–19-year-olds); however, there is evidence that hacking behaviours could start as early at nine years of age [37]. Furthermore, when conceptualising youth populations, there is some evidence that the risk-taking typically associated with adolescence is in some part caused by brain maturation processes that continue into the mid-20s [1], therefore moving the conceptual age of adulthood to approximately 25. Therefore, extending the age range could test the age–crime curve relationship and the hypothesised natural desistance of the majority of hackers by their mid-20s [25,53,54].

Fifth, future studies may consider the incorporation of other factors, such as victimisation leading to perpetration [85], and a combined TPB model of both human factors and technical factors to concurrently assess and parse to what extent human and technical drivers are associated with criminal hacking.

Sixth, whilst this study was conducted in nine European countries, a limitation of this study is that the survey did not include former Soviet satellite countries, where organised criminal hacking (in groups) is more prevalent; arguably, this would be a very interesting follow-on study.

Finally, a future study could replicate this study with a smaller but probabilistic sample to assess to what extent our findings are generalisable to the wider population. By collecting these samples within multiples countries, future studies can definitively assess differences across countries.

8.3. Application of Findings

A unique contribution of this study was to determine that gender and offline deviant behaviours are strong predictors, being significantly associated with the majority of the constructs and covariates within this model, including hacking behaviour and intention, constructs within the TPB conceptual framework, as well as demographics and human

factors. This is a unique finding, as the explanatory power of these predictors was assessed concurrently against other demographic variables and human factors. Therefore, this finding suggests that these two factors (gender and involvement in offline deviant behaviour) may prove salient mechanisms for intervention programmes for those already engaged in hacking behaviours. These findings have significant implications for both law enforcement and intervention mechanisms. Firstly, these findings indicate that there is little sharp division between offline and online crime; rather, these findings point towards a general propensity for engaging in risky and criminal behaviour. This suggests a significant shift in how cybercrime, in particular technical cybercrimes like hacking, are conceptualised, investigated, and legislated. Secondly, this finding suggests that targeted interventions should be directed at specific at-risk populations, in this case, delinquent young adult males.

With regard to reducing hacking intentions, and thereby the occurrence of the actual behaviour, aside from offline delinquency and gender, as previously identified, the adapted TPB Model of Criminal Hacking as a framework suggests there are many possible vectors to target to stage interventions, including directly addressing the cognitive processes themselves (TPB constructs: attitudes, subjective norms, and perceived behavioural control), as well as the factors significantly associated with these cognitive processes, including risk-seeking, online disinhibition, and age. A key observation (shown in Figure 1) is that the strongest predictor of intention within the TPB framework is the SN of parents. Therefore, educating parents about online risk may prove to be a particularly effective intervention methodology, in terms of education and awareness-raising initiatives.

Also, through the subjective norms of friends and internal attitudes and beliefs, the intention to hack could be further influenced, i.e., utilising the combined effect of TPB cognitive constructs. Therefore, it is imperative at the policy level to design education and awareness-raising initiatives for young people to be deployed within a formal educational setting. These initiatives should focus on educating young people about the risks associated with online crime; fostering appropriate beliefs and attitudes towards criminal behaviour online; and upskilling and encouraging young people to use technology in safe and legal ways. Furthermore, widespread awareness-raising campaigns should also focus on educating young people on these key issues. For example, the findings of this paper were translated into education and awareness-raising materials and were disseminated broadly through Europe, launched as part of Safer Internet Day 2023 [86].

9. Conclusions

Despite the complexity of the behaviour of interest (hacking), this study has formulated a powerful predictive model of youth hacking intention (accounting for 38.8% of the variance) and behaviour (accounting for 33.6% of the variance). Overall, the TPB conceptual framework proved to be a powerful paradigm to form an adapted TPB model to predict hacking intention and behaviour, incorporating and importantly being able to concurrently assess different cyberpsychological, psychological, and criminological factors. With regards to application, this approach has identified multiple possible vectors with which to stage interventions in relation to human factors, either to tailor interventions to most at-risk groups (e.g., older teen males) or to intervene on strong predictors of behaviours (e.g., parental attitudes or teens known to be engaging in offline deviancy).

Author Contributions: Conceptualisation, M.P.A., J.C.D. and M.W.; Methodology, M.P.A., J.C.D., M.W. and K.P.; Formal Analysis, K.S.P., M.W., M.P.A., J.C.D. and K.P.; Investigation, M.P.A., J.C.D., K.P. and R.R.F.; Data Curation, K.P., R.R.F., M.P.A. and J.C.D.; Writing—Original Draft, M.P.A. and K.P.; Writing—Review and Editing, M.P.A., K.P., J.C.D., M.W. and K.S.P.; Visualisation, K.S.P., K.P., M.P.A. and J.C.D.; Supervision, M.P.A. and J.C.D.; Administration, J.C.D., M.P.A. and K.P.; Funding Acquisition, M.P.A. and J.C.D. All authors have read and agreed to the published version of the manuscript.

Funding: This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement [No 883543].

Institutional Review Board Statement: This study was conducted in accordance with the ethical standards of the British Psychological Association (BPS); permissions were granted by the UEL ethics committee (ETH2021-0065).

Informed Consent Statement: Participants were required to indicate that they had read the consent form and had consented to take part before progressing to the study questions. If participants did not consent to take part they were exited from the survey. All participants were provided with a debrief form upon completion of the study.

Data Availability Statement: Data are unavailable due to privacy and ethical restrictions.

Acknowledgments: This research was completed by CC-DRIVER, 'Combating Cyber Criminality by Understanding Human and Technical Drivers', partners at University of East London in collaboration with Michel Walrave (Research Group MIOS, University of Antwerp) and Koen Ponnet (Research Group imec-mict, Ghent University). The authors would like to thank the other partners of the CC-DRIVER consortium supporting the development of this study and the on-going CC-DRIVER research programme.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Johnson, S.B.; Blum, R.W.; Giedd, J.N. Adolescent maturity and the brain: The promise and pitfalls of neuroscience research in adolescent health policy. *J. Adolesc. Health* **2009**, *45*, 216–221. [CrossRef]
2. Odgers, C.L.; Jensen, M.R. Adolescent development and growing divides in the digital age. *Dialogues Clin. Neurosci.* **2022**, *22*, 143–149. [CrossRef]
3. Rideout, V.; Peebles, A.; Mann, S.; Robb, M.B. Common Sense Census: Media Use by Tweens and Teens, 2021. Common Sense. 2022. Available online: https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf (accessed on 27 September 2023).
4. Davidson, J.; Aiken, M.; Phillips, K.; Farr, R. 2022 Research Report. CC-DRIVER. 2022. Available online: https://www.ccdriver-h2020.com/publications (accessed on 11 September 2023).
5. Logos, K.; Rubinshtein, S.; Brewer, R.; Whitten, T.; Cale, J.; Holt, T.; Goldsmith, A. *South Australian Digital Youth Survey Research Report: Year 3 Results*; University of Adelaide: Adelaide, Australia, 2021. Available online: https://researchoutput.csu.edu.au/en/publications/south-australian-digital-youth-survey-research-report-year-3-resu#:~:text=Access%20to%20Document-,https://digital.library.adelaide.edu.au/dspace/handle/2440/134755,-Fingerprint (accessed on 1 January 2020).
6. Cioban, S.; Lazăr, A.R.; Bacter, C.; Hatos, A. Adolescent deviance and cyber-deviance. A systematic literature review. *Front. Psychol.* **2021**, *12*, 748006. [CrossRef]
7. Young, S.; Greer, B.; Church, R. Juvenile delinquency, welfare, justice and therapeutic interventions: A global perspective. *BJPsych Bull.* **2017**, *41*, 21–29. [CrossRef] [PubMed]
8. Payne, B.K. Defining cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 3–25. [CrossRef]
9. Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sci.* **2022**, *2*, 379–398. [CrossRef]
10. McGuire, M.; Dowling, S. Cybercrime: A Review of the Evidence: Summary of Key Findings and Implications. Home Office. 2013. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed on 20 September 2023).
11. Council of Europe. Convention on Cybercrime. European Treaty Series No. 185. 2001, pp. 1–22. Available online: https://rm.coe.int/1680081561 (accessed on 18 September 2023).
12. Viano, E.C. Cybercrime: Definition, typology, and criminalization. In *Cybercrime, Organized Crime, and Societal Responses*; Viano, E.C., Ed.; Springer International Publishing: Cham, Switzerland, 2017; pp. 3–22.
13. Brewer, R.C.; Cale, J.; Goldsmith, A.; Holt, T. Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. *Int. J. Cyber Criminol.* **2018**, *12*, 115–132. [CrossRef]
14. Schell, B. Internet addiction and cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 679–703. [CrossRef]
15. Aiken, M.; Davidson, J.; Amann, P. Youth Pathways into Cybercrime. Paladin Capital Group. 2016. Available online: https://www.paladincapgroup.com/wp-content/uploads/2016/11/Pathways-White-Paper-US-final-1.pdf (accessed on 17 September 2023).

16. NCA [National Crime Agency]. Pathways into Cyber Crime. National Crime Agency Unit/Prevent Team. 13 January 2017. Available online: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file (accessed on 17 September 2023).
17. Holt, T.J.; Bossler, A. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*; Routledge: Abingdon, UK, 2015. [CrossRef]
18. Back, S.; Soor, S.; LaPrade, J. Juvenile hackers: An empirical test of self-control theory and social bonding theory. *Int. J. Cybersecur. Intell. Cybercrime* **2018**, *1*, 40–55. [CrossRef]
19. Bachmann, M. The risk propensity and rationality of computer hackers. *Int. J. Cyber Criminol.* **2010**, *4*, 643–656.
20. Chua, Y.T.; Holt, T.J. A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Vict. Offenders* **2016**, *11*, 534–555. [CrossRef]
21. Jordan, T.; Taylor, P. A sociology of hackers. *Sociol. Rev.* **1998**, *46*, 757–780. [CrossRef]
22. Steinmetz, K.; Gerber, J. "It doesn't have to be this way": Hacker perspectives on privacy. *Soc. Justice* **2015**, *41*, 29–51. Available online: https://www.jstor.org/stable/24361631 (accessed on 16 September 2023).
23. Turgeman-Goldschmidt, O. Hackers' accounts: Hacking as a social entertainment. *Soc. Sci. Comput. Rev.* **2005**, *23*, 8–23. [CrossRef]
24. Turgeman-Goldschmidt, O. Meanings that hackers assign to their being a hacker. *Int. J. Cyber Criminol.* **2008**, *2*, 382–396. Available online: https://www.cybercrimejournal.com/pdf/Orlyijccdec2008.pdf (accessed on 20 September 2023).
25. Yar, M. Computer hacking: Just Another case of juvenile delinquency? *Howard J. Crim. Justice* **2005**, *44*, 387–399. [CrossRef]
26. Zhang, L.; Young, R.; Prybutok, V. A comparison of the inhibitors of hacking vs. shoplifting. In *Evolutionary Concepts in End User Productivity and Performance: Applications for Organizational Progress*; Clarke, S., Ed.; IGI Global: Hershey, PA, USA, 2008; pp. 63–77. [CrossRef]
27. Bossler, A. Contributions of criminological theory to the understanding of cybercrime offending and victimization. In *The Human Factor of Cybercrime*; Leukfeldt, R., Holt, T.J., Eds.; Routledge: Abingdon, UK, 2019; pp. 29–59.
28. Ajzen, I. From intentions to actions: A theory of planned behavior. In *Action Control*; Kuhl, J., Beckmann, J., Eds.; SSSP Springer Series in Social Psychology; Springer: Berlin/Heidelberg, Germany, 1985; pp. 11–39. [CrossRef]
29. Ajzen, I.; Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*; Prentice-Hall: Upper Saddle River, NJ, USA, 1980.
30. Owen, K. Motivation and Demotivation of Hackers in the Selection of a Hacking Task: A Contextual Approach. Ph.D. Thesis, McMaster University, Hamilton, ON, Canada, 2016.
31. Jeong, J.; Mihelcic, J.; Oliver, G.; Rudolph, C. Towards an improved understanding of human factors in cybersecurity. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 338–345. [CrossRef]
32. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
33. Heirman, W.; Walrave, M. Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behavior. *Psicothema* **2012**, *24*, 614–620. Available online: https://www.psicothema.com/pdf/4062.pdf (accessed on 26 September 2023).
34. Walrave, M.; Heirman, W.; Hallam, L. Under pressure to sext? Applying the theory of planned behaviour to adolescent sexting. *Behav. Inf. Technol.* **2014**, *33*, 86–98. [CrossRef]
35. Chng, S.; Lu, H.Y.; Kumar, A.; Yau, D. Hacker types, motivations and strategies: A comprehensive framework. *Comput. Hum. Behav. Rep.* **2022**, *5*, 100167. [CrossRef]
36. EUROPOL. *Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis*; European Union Agency for Law Enforcement Cooperation: The Hague, The Netherlands, 2020. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf (accessed on 20 September 2023).
37. NCA. Rise in School Cyber Crime Attacks Sparks NCA Education Drive. National Crime Agency. 17 January 2022. Available online: https://www.nationalcrimeagency.gov.uk/news/rise-in-school-cyber-crime-attacks-sparks-nca-education-drive (accessed on 20 September 2023).
38. Armitage, C.J.; Conner, M. Efficacy of the theory of planned behaviour: A meta-analytic review. *Br. J. Soc. Psychol.* **2001**, *40*, 471–499. [CrossRef]
39. Holt, T.J.; Brewer, R.; Goldsmith, A. Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime. *Deviant Behav.* **2019**, *40*, 1144–1156. [CrossRef]
40. Matza, D. *Delinquency & Drift*; Wiley: Hoboken, NJ, USA, 1964.
41. Holt, T.J. Computer hacking and the hacker subculture. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 725–742. [CrossRef]
42. Staggs, S.; McMichael, S.L.; Kwan, V.S.Y. Wishing to be like the character on screen: Media exposure and perception of hacking behavior. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2020**, *14*, 4. [CrossRef]
43. The Mentor. The Conscience of a Hacker. *Phrack* **1986**, *1*, 15. Available online: http://phrack.org/issues/7/3.html (accessed on 28 January 2024).
44. Steinberg, L. *Adolescence*, 12th ed.; McGraw Hill Education: Maidenhead, UK, 2020.
45. Whitbourne, S.K. *Life Span Development*; American Psychological Association: New York, NY, USA, 2012.
46. Spear, L.P. The adolescent brain and age-related behavioral manifestations. *Neurosci. Biobehav. Rev.* **2000**, *24*, 417–463. [CrossRef] [PubMed]

47. Pratt, T.C.; Cullen, F.T.; Sellers, C.S.; Thomas Winfree, L.J., Jr.; Madensen, T.D.; Daigle, L.E.; Fearn, N.C.; Gau, J.M. The empirical status of social learning theory: A meta-analysis. *Justice Q.* **2010**, *27*, 765–802. [CrossRef]
48. Bossler, A.M.; Burruss, G.W. The general theory of crime and computer hacking: Low self-control hackers? In *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*; Holt, T.J., Schell, B.H., Eds.; IGI Global: Hershey, PA, USA, 2011; pp. 38–67. [CrossRef]
49. Skinner, W.F.; Fream, A.M. A social learning theory analysis of computer crime among college students. *J. Res. Crime Delinq.* **1997**, *34*, 495–518. [CrossRef]
50. Holt, T.J. Examining the role of technology in the formation of deviant subcultures. *Soc. Sci. Comput. Rev.* **2010**, *28*, 466–481. [CrossRef]
51. Holt, T.J. Subcultural evolution? Examining the influence of on and off-line experiences on deviant subcultures. *Deviant Behav.* **2007**, *28*, 171–198. [CrossRef]
52. Schell, B.H.; Dodge, J.L. *The Hacking of America: Who's Doing it, Why, and How*; Greenwood Publishing Group, Inc.: Westport, CT, USA, 2002.
53. Sterling, B. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*; Penguin: London, UK, 1994.
54. Taylor, P. *Hackers: Crime and the Digital Sublime*, 1st ed.; Routledge: Abingdon, UK, 1999. [CrossRef]
55. Gilboa, N. Elites, lamers, narcs, and whores: Exploring the computer underground. In *Wired_Women*; Cherny, L., Weise, E.R., Eds.; Seal Press: Cypress, CA, USA, 1996; pp. 98–113.
56. Marcum, C.D.; Higgins, G.E.; Ricketts, M.L.; Wolfe, S.E. Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behav.* **2014**, *35*, 581–591. [CrossRef]
57. Barbieri, D.; Caisl, J.; Karu, M.; Lanfredi, G.; Mollard, B.; Peciukonis, V.; Salanauskaitė, L. *Gender Equality Index 2020: Digitalisation and the Future of Work*; European Institute for Gender Equality (EIGE): Vilnius, Lithuania, 2020. Available online: https://eige.europa.eu/sites/default/files/documents/mhaf20001enn_002.pdf (accessed on 20 September 2023).
58. Heimer, K.; De Coster, S. Crime and gender. In *International Encyclopedia of the Social & Behavioural Sciences*; Smelser, N.J., Baltes, P.B., Eds.; Elsevier Science Ltd.: Amsterdam, The Netherlands, 2001; pp. 2918–2921.
59. Gottfredson, M.R.; Hirschi, T. *A General Theory of Crime*; Stanford University Press: Redwood City, CA, USA, 1990.
60. Holt, T.J.; Bossler, A.M.; May, D.C. Low self-control, deviant peer associations, and juvenile cyberdeviance. *Am. J. Crim. Justice* **2012**, *37*, 378–395. [CrossRef]
61. Udris, R. Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *Int. J. Cyber Criminol.* **2016**, *10*, 127–146. Available online: http://www.cybercrimejournal.com/Udrisvol10issue2IJCC2016 (accessed on 26 September 2023).
62. Grasmick, H.G.; Tittle, C.R.; Bursik, R.J., Jr.; Arneklev, B.J. Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *J. Res. Crime Delinq.* **1993**, *30*, 5–29. [CrossRef]
63. Suler, J. The online disinhibition effect. *Cyberpsychology Behav.* **2004**, *7*, 321–326. [CrossRef]
64. Soudijn, M.R.J.; Zegers, B.C.H.T. Cybercrime and virtual offender convergence settings. *Trends Organ. Crime* **2021**, *15*, 111–129. [CrossRef]
65. Udris, R. Psychological and social factors as predictors of online and offline deviant behavior among Japanese adolescents. *Deviant Behav.* **2017**, *38*, 792–809. [CrossRef]
66. Goldsmith, A.; Brewer, R. Digital drift and the criminal interaction order. *Theor. Criminol.* **2014**, *19*, 112–130. [CrossRef]
67. Cale, J.; Whitten, T.; Brewer, R.; de Vel-Palumbo, M.; Goldsmith, A.; Holt, T. *South Australian Digital Youth Survey Research Report: Year 1 Results*; University of Adelaide: Adelaide, Australia, 2019.
68. Sabillon, R.; Cavaller, V.; Cano, J.; Serra-Ruiz, J. Cybercriminals, cyberattacks and cybercrime. In Proceedings of the 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, 12–14 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–9. [CrossRef]
69. Ajzen, I. Design and evaluation guided by the theory of planned behavior. In *Social Psychology Evaluation*; Mark, M.M., Donaldson, S.I., Campbell, B.C., Eds.; The Guilford Press: New York, NY, USA, 2011; pp. 74–100.
70. Udris, R. Cyberbullying among high school students in Japan: Development and validation of the online disinhibition scale. *Comput. Hum. Behav.* **2014**, *41*, 253–261. [CrossRef]
71. Sanches, C.; Gouveia-Pereira, M.; Marôco, J.; Gomes, H.; Roncon, F. Deviant behavior variety scale: Development and validation with a sample of Portuguese adolescents. *Psicol. Reflexão Crítica* **2016**, *29*, 31–38. [CrossRef]
72. Muthén, L.K.; Muthén, B.O. *Mplus User's Guide. Version 8.7*; Muthén & Muthén: Los Angeles, CA, USA, 2021. Available online: https://www.statmodel.com/download/usersguide/MplusUserGuideVer_8.pdf (accessed on 20 September 2023).
73. Brown, T.A. *Confirmatory Factor Analysis for Applied Research*; The Guilford Press: New York, NY, USA, 2006.
74. Kline, R.B. *Principles and Practices of Structural Equation Modelling*, 2nd ed.; The Guilford Press: New York, NY, USA, 2005.
75. Bentler, P.M. Comparative fit indexes in structural models. *Psychol. Bull.* **1990**, *107*, 238–246. [CrossRef]
76. Tucker, L.R.; Lewis, C. Reliability coefficients for maximum likelihood factor-analysis. *Psychometrika* **1973**, *38*, 1–10. [CrossRef]
77. Steiger, J.H. Structural model evaluation and modification: An interval estimation approach. *Multivar. Behav. Res.* **1990**, *25*, 173–180. [CrossRef]
78. Byrne, B.M. *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*; Lawrence Erlbaum Associates Publishers: Mahwah, NJ, USA, 2001.

79. Hu, L.; Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struct. Equ. Model.* **1999**, *6*, 1–55. [CrossRef]
80. Ponnet, K. Financial stress, parent functioning and adolescent problem behavior: An actor-partner interdependence approach to family stress processes in low-, middle-, and high-income families. *J. Youth Adolesc.* **2014**, *43*, 1752–1769. [CrossRef] [PubMed]
81. Holt, T.J.; Navarro, J.N.; Clevenger, S. Exploring the moderating role of gender in juvenile hacking behaviors. *Crime Delinq.* **2020**, *66*, 1533–1555. [CrossRef]
82. Goldsmith, A.; Wall, D.S. The seductions of cybercrime: Adolescence and the thrills of digital transgression. *Eur. J. Criminol.* **2019**, *19*, 98–117. [CrossRef]
83. Moore, G.F.; Rothwell, H.; Segrott, J. An exploratory study of the relationship between parental attitudes and behaviour and young people's consumption of alcohol. *Subst. Abus. Treat. Prev. Policy* **2010**, *5*, 6. [CrossRef]
84. Wachs, S.; Wright, M.F. The moderation of online disinhibition and sex on the relationship between online hate victimization and perpetration. *Cyberpsychol. Behav. Soc. Netw.* **2019**, *22*, 300–306. [CrossRef]
85. Logan-Greene, P.L.; Nurius, P.S.; Herting, J.R.; Walsh, E.; Thompson, E.A. Violent victimization and perpetration: Joint and distinctive implications for adolescent development. *Vict. Offenders* **2010**, *5*, 329–353. [CrossRef]
86. UK Safer Internet Centre. Safer Internet Day 2023. UK Safer Internet Centre. 2022. Available online: https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2023 (accessed on 27 September 2023).