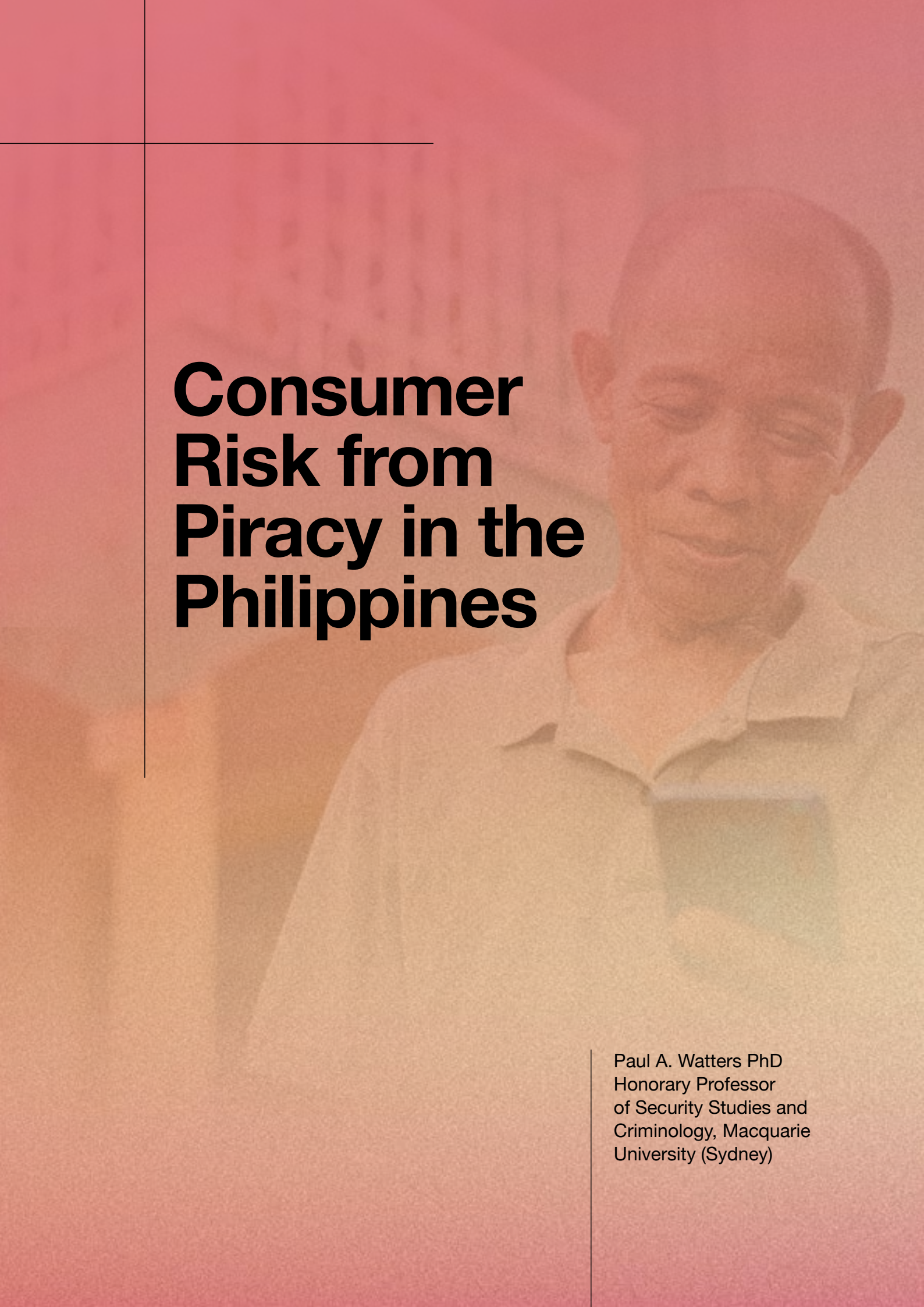
Consumer Risk from Piracy in the Philippines

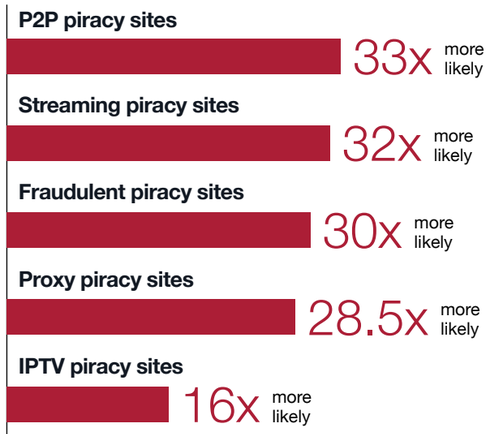


Paul A. Watters PhD
Honorary Professor
of Security Studies and
Criminology, Macquarie
University (Sydney)

Consumer Risk from Piracy in the Philippines

Executive Summary

Filipino consumers are 27.90 times more likely to encounter a cyber threat when using piracy sites:



Filipino consumers who access piracy sites and services are at severe risk of cyber threats from a range of criminal groups operating in an increasingly complex and challenging geopolitical environment. The Philippines, with its rapidly growing internet penetration and thriving digital economy, has become an attractive target for cybercriminals who exploit digital piracy to spread malware, viruses, and other cyber threats. These piracy sites, often disguised as legitimate platforms, harbor concealed malware that poses a significant threat to consumers. By visiting these sites, Filipinos inadvertently expose themselves to risks such as personal information theft, ransomware attacks, and sextortion.

Key Findings

33x

Filipinos have up to a 33.00 times greater chance of encountering a cyber threat on the most popular piracy sites compared to legal film/TV websites.

15

Some piracy sites have up to 15 unique cyber threats on a single site, including malware and phishing.

Zero

Zero day cyber attacks mean rapid action through site blocking of piracy sites is essential to reduce the cyber risk of Filipino consumers.

The aim of this study was to quantify the cyber risks faced by Filipino consumers who engage with digital piracy websites, including fraudulent sites, illegal streaming services, proxy sites, P2P sites, or IPTV platforms. The findings reveal an alarming set of cyber risks: when compared to a set of control sites comprising the most popular 30 legal film/TV sites in the Philippines, the relative risk was 33.00 times greater for P2P sites, 32.00 times greater for streaming sites, 30.00 times greater for fraudulent sites, 16.00 times greater for IPTV sites, and 28.50 times greater for proxy sites. In practical terms, this means that Filipino consumers are 27.90 times more likely to encounter a cyber threat when using piracy sites compared to mainstream websites, on average; an extraordinary result that underscores the gravity of the situation.

To mitigate the elevated cyber risks, this report recommends the following actions:

1. **Enact proportionate and transparent site blocking laws that will target piracy sites and services:** Blocking access to these sites could significantly reduce exposure to cyber threats, especially given that many piracy sites popular in the Philippines are hosted outside the country. However, this measure can only be implemented once House Bill 7600, and Senate Bills 2150, 2385, 2645, and 2651 are enacted into law, ensuring the proposed administrative process is carried out transparently and with due regard to consumer rights.

2. **Increase funding for Filipino law enforcement to enhance digital forensics and incident response capabilities:** Given the heightened cyber threats linked to digital piracy, it is crucial to bolster the capabilities of Filipino law enforcement in digital forensics and incident response, ensuring they are equipped to handle the evolving cyber threat landscape, as described in the National Cybersecurity Plan 2022.

3. **Develop a national awareness and education campaign:** There is an urgent need for a comprehensive national campaign in the Philippines to educate consumers about the cyber risks associated with using piracy sites or services, emphasizing safe online practices and promoting legal alternatives.

These recommendations offer a sensible and proportional response to a serious threat to consumer safety in the Philippines, particularly in an era where data breaches and large-scale identity theft are increasingly common on a global scale.

Contents

Consumer Risk from Piracy in the Philippines 5

Introduction

01

What is digital piracy?

How widespread is digital piracy in the Philippines?

What are the social and economic consequences of digital piracy?

What are the consumer risks of digital piracy?

What is the consumer threat model for piracy?

An evolving threat model for digital piracy.

What is the financial situation of consumers in the Philippines?

Why are Filipino consumers attractive targets for cyber threats?

What are the protective factors in terms of cyber policy and regulatory responses?

Introduction

Digital piracy in the Philippines has far-reaching repercussions, particularly in the realm of cybersecurity. Filipino consumers are increasingly turning to illegal streaming platforms, torrent sites[1], and other forms of digital piracy – a Media Partners Asia study found that the Philippines was second only to Indonesia in the number of consumers who visit piracy sites, with rates increasing to 70% according to YouGov data[2].

While doing so may seem to provide free or lower cost access to entertainment, consumers unwittingly expose themselves to a host of cyber threats. These platforms are designed to deliver malware, viruses, and other malicious software designed to compromise user security.

The consequences of engaging with such platforms are severe, including personal data theft, financial loss, and the potential hijacking of personal devices. In a country where digital infrastructure is rapidly evolving – such as the $288m national broadband program[3] – the cybersecurity risks associated with digital piracy represent a significant and growing threat to consumer safety.

The study involves an in-depth examination of consumer risk, identification of existing vulnerabilities, and a comprehensive assessment of these risks. Understanding these factors is crucial for developing effective risk mitigation strategies, including regulatory reforms, resource allocation for law enforcement, and consumer education initiatives. Through an empirical approach, the research seeks to provide scientific insights into the central question: what is the cyber risk for consumers in the Philippines who visit piracy sites, and how does risk quantification inform a policy response?

What is digital piracy?

Digital piracy refers to the unauthorized use, reproduction, distribution, or downloading of copyrighted materials such as movies, music, software, or books without the permission of the rightful owner[4]. This illegal activity often occurs through various platforms, including torrent sites, illegal streaming services, and file-sharing networks.

Digital piracy undermines the intellectual property rights of creators and companies, leading to significant financial losses in industries like entertainment and software[5]. Beyond the economic impact, digital piracy is frequently linked to cybersecurity risks, as many piracy websites and files are laced with malware, exposing users to potential cyber threats such as identity theft, ransomware, and data breaches[6]. Despite efforts to combat it, digital piracy remains a widespread issue, fueled by the growing demand for free access to digital content[7].

The main sources of digital piracy content include[8]:

1. **P2P Sites:** Platforms like The Pirate Bay and other BitTorrent websites are popular for sharing and downloading links to pirated content, including movies, music, software, and games. Users upload and download files through a peer-to-peer (P2P) network, which facilitates the distribution of copyrighted material without authorization, relying on either centralized trackers or magnet links to identify the location of content.
2. **Illegal Streaming Sites:** Websites that stream movies, TV shows, sports events, and other video content without proper licensing are a major source of digital piracy. These platforms often resemble legitimate streaming services but operate illegally, providing free access to copyrighted content.
3. **IPTV Piracy Services:** Some Internet Protocol Television (IPTV) services offer unauthorized access to live television channels, pay-per-view events, and on-demand content. These services often charge a subscription fee but operate without the necessary rights or licenses, making them a source of pirated content.
4. **Proxy Sites:** Proxy sites play a significant role in digital piracy by allowing users to access pirated content while bypassing restrictions and anonymity. These sites act as intermediaries, masking the user's IP address and enabling access to blocked or restricted websites, including those hosting pirated content.
5. **Rogue Websites and Fraudulent Sites:** These websites mimic legitimate platforms but are set up specifically to distribute pirated content, often bundling it with malware or other malicious software. Users may inadvertently access these sites through deceptive ads or links.

These sources contribute to the widespread availability of pirated content, complicating efforts to enforce copyright laws and protect intellectual property rights[9].

Digital piracy - through avenues like torrent sites, illegal streaming services, file-sharing networks, and rogue websites - significantly undermines content creators' rights by depriving them of revenue and diminishing the value of their intellectual property[10].

These platforms facilitate the unauthorized distribution of copyrighted material, leading to substantial financial losses in industries such as entertainment, software, and publishing. For distributors, the legal consequences are severe, including potential fines, civil lawsuits, and imprisonment under copyright laws.

However, the widespread availability of pirated content further complicates efforts to protect creators' rights and uphold intellectual property laws. The impact of digital piracy on consumers can be severe - pirated content often comes bundled with hidden malware, which can infect users' devices when they download or stream from illegal sites[11].

This malware can lead to a range of issues, including unauthorized access to personal files, and annoying, hard-to-remove pop-ups that deliver more malware[12]. More critically, consumers may fall victim to identity theft if the malware captures sensitive information such as passwords, credit card numbers, or personal identification details. These credentials are often bundled and sold on the wholesale black market[13].

Additionally, some pirated content is used as a gateway for more sophisticated cyber attacks, like ransomware[14], which can lock users out of their devices until a ransom is paid. Engaging with pirated content thus exposes consumers to a high risk of financial loss, privacy violations, and long-term damage to their digital security.

How widespread is digital piracy in the Philippines?

Digital piracy is notably widespread in the Philippines, driven by several factors including high demand for free or low-cost content, relatively low levels of digital literacy among some segments of the population, and the availability of pirated content through various online platforms.

According to the Philippine Institute for Development Studies (PIDS), digital literacy is lowest amongst 10-14 year olds, and those 65 years and above[15]. Sitting alongside this are some of the highest social media penetration rates, but only 30 percent of the population have digital skills[16].

A recent YouGov survey indicated that 70 percent of the population had consumed pirated content through a streaming platform[17]. With the further expansion of broadband, the country has a large and growing internet user base, with many Filipinos accessing pirated movies, music, software, and TV shows via torrent sites, illegal streaming platforms, and social media channels.

Enforcement of copyright laws in the country has been challenging, with limited resources for cracking down on piracy and low public awareness of the legal and cybersecurity risks associated with it. On the other hand, some 7.1 percent of GDP depends on the creative industries; there is a clear economic necessity to do more[18].

Pirated content is easily accessible, often shared through social media and messaging apps, making it difficult to regulate and control. This has made the Philippines one of the hotspots for digital piracy in the region, with significant implications for the entertainment industry, software companies, cybersecurity within the country, and digital trade within the region[19].

70%

of the population have consumed pirated content through a streaming platform.

only

30%

of the population have digital skills.

Digital piracy has wide-ranging social and economic consequences, as described in the following sections.

What are the social and economic consequences of digital piracy?

SOCIAL CONSEQUENCES

Digital piracy erodes the cultural value of creative works by diminishing their perceived worth, which can lead to reduced investment in new and diverse content. It negatively impacts artists and creators by depriving them of potential income, which in turn can stifle creativity and discourage emerging talent. These are clear social harms, and the extent of the harm is measurable[20]. Additionally, as piracy affects the profitability of content producers, it may result in less availability of legal content, particularly in regions where piracy is prevalent[21].

Digital piracy can undermine cultural diversity by prioritizing mainstream content and limiting the exposure of diverse cultural expressions. Financial losses from piracy can hinder the production and distribution of niche or culturally diverse content, as creators may struggle economically and investors may shy away from funding less commercially safe projects.

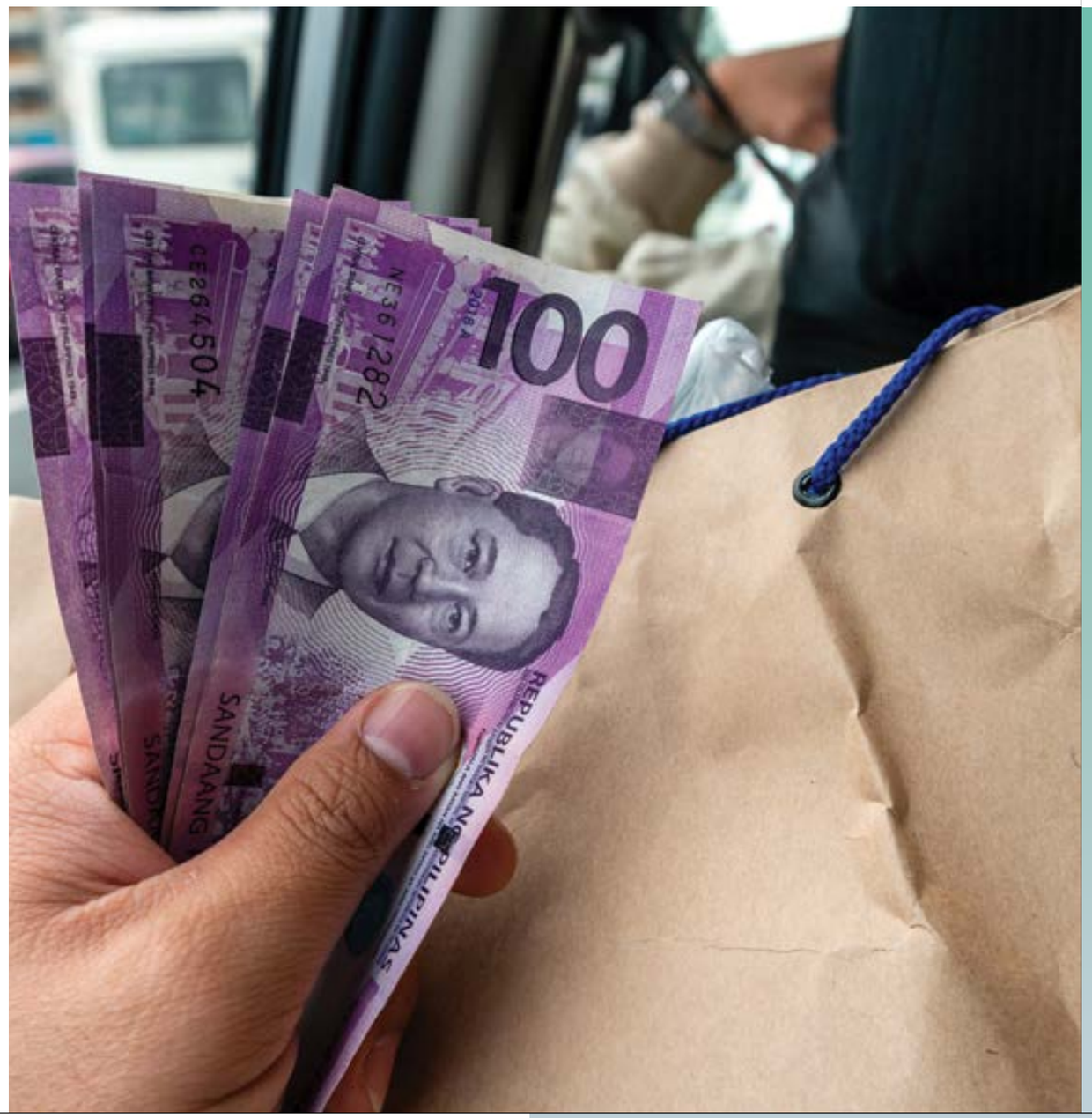
As a result, piracy can reduce the variety of cultural perspectives available and diminish the richness of cultural representation in the media[22].

In the Philippines, digital piracy has specific implications for cultural diversity. The widespread availability of pirated content can overshadow local and indigenous media, making it harder for Filipino creators and diverse cultural expressions to gain visibility and financial support. This can stifle the growth of the local entertainment industry and limit the representation of Filipino culture in global media. Additionally, the financial strain on local creators and producers from piracy can lead to a preference for mainstream, commercially safe content over innovative or culturally diverse projects. As a result, piracy can contribute to a homogenization of media and diminish the rich tapestry of Filipino cultural diversity.

ECONOMIC CONSEQUENCES

Digital piracy has significant economic consequences, particularly impacting industries such as film, music, and software that rely heavily on intellectual property to generate revenue. The most immediate effect is revenue loss, as pirated content reduces the potential earnings from legitimate sales and subscriptions. This loss in revenue can be substantial, affecting total profitability and financial stability of these industries. To combat piracy, companies often incur additional costs related to legal actions, enforcement of digital rights management (DRM), and the development of anti-piracy technologies, which can further strain their budgets[23]. These financial pressures can lead to job losses, as companies may need to reduce staff or cut back on investments in production and innovation. Moreover, the reduced profitability can discourage investment in new projects, particularly in sectors where piracy is most rampant. Thus, digital piracy not only diminishes the income of content creators and distributors but also has a ripple effect that can negatively impact employment and innovation within the affected industries.

To protect digital assets from piracy, businesses often face significant financial and operational challenges. Implementing robust anti-piracy measures involves substantial investment in security technologies, such as digital rights management (DRM) systems, encryption, and watermarking tools – in recent years, even the blockchain has been suggested[24]. These technologies are designed to prevent unauthorized access and distribution of digital content, but they require ongoing maintenance and updates to remain effective and can be very costly.



These costs may then trigger a rise in prices, leading to consumer dissatisfaction. Additionally, businesses may need to invest in specialized personnel to manage and monitor these systems, conduct regular audits, and respond to potential breaches. The costs associated with these measures can be particularly burdensome for smaller enterprises, potentially diverting funds from other critical areas such as supporting emerging artists. Furthermore, maintaining an effective anti-piracy strategy often requires continuous adaptation to counter new piracy tactics, adding to the long-term financial strain. Thus, while protecting digital assets from piracy is essential for safeguarding revenue and intellectual property, the associated costs and resource allocation are significant challenges for the creative economy.

In addition to direct losses in the content-producing industries, ancillary industries that support film and television production also feel the economic strain of digital piracy. These industries—such as set construction, catering, location scouting, equipment rental, and post-production services—rely on healthy, ongoing production schedules that can be curtailed when studios or production houses face financial challenges due to piracy. When film and TV projects suffer from reduced budgets caused by piracy-related revenue losses, they cut back on these essential services. As a result, jobs are lost not only in the primary creative industries but across a broader ecosystem of businesses and workers that contribute to production. This ripple effect extends the economic damage of piracy far beyond the studios themselves, weakening local economies and stifling innovation in industries that depend on a thriving film and television sector.

What are the consumer risks of digital piracy?

Digital piracy presents several risks to consumers that can significantly impact their digital experiences and personal security. One major risk is exposure to malware, as pirated content is often distributed by cybercriminals, increasing the likelihood of downloading malicious software such as viruses or ransomware that can damage devices and compromise personal information.

In a study funded by the NSA[25], doubling the time spent on a piracy site led to a 20 percent increase in exposure to malware, excluding adware. The study also found that users of piracy sites were less likely to use anti-virus software; if a user then connected a compromised device to a corporate network, say through a VPN, the consequences could be significant for their employer[26].

Additionally, pirated content like “cams” may suffer from poor quality and reliability, leading to substandard viewing or usage experiences. Consumers may also face privacy concerns, as sites offering pirated content can exploit personal information for malicious purposes, including identity theft or unauthorized data collection.

This is not a hypothetical risk – the recent exposure of the details of 10 million users of a z-library copycat site illustrates the dangers[27].

While accessing pirated content might seem appealing for its cost savings, the associated risks can lead to significant negative consequences for consumers in terms of security, quality, and ethical implications. Organized crime plays a significant role in digital piracy, often operating sophisticated networks that facilitate the distribution of pirated content[28] - a phenomenon known as criminal convergence[29].

Such criminal organizations exploit piracy, money laundering, drug trafficking, and human trafficking to generate substantial illicit profits.

They may use piracy as a cover for more serious crimes, as the distribution of pirated content often involves complex, clandestine networks that can obscure other illicit activities, such as distributing child exploitation material[30].

Furthermore, the financial gains from piracy can fund further criminal enterprises and violence, perpetuating a cycle of crime.

The involvement of organized crime in digital piracy not only exacerbates the economic and social impact of piracy but also poses serious threats to law enforcement and public safety, complicating efforts to combat both piracy and the broader criminal activities associated with it.

What is the consumer threat model for piracy?

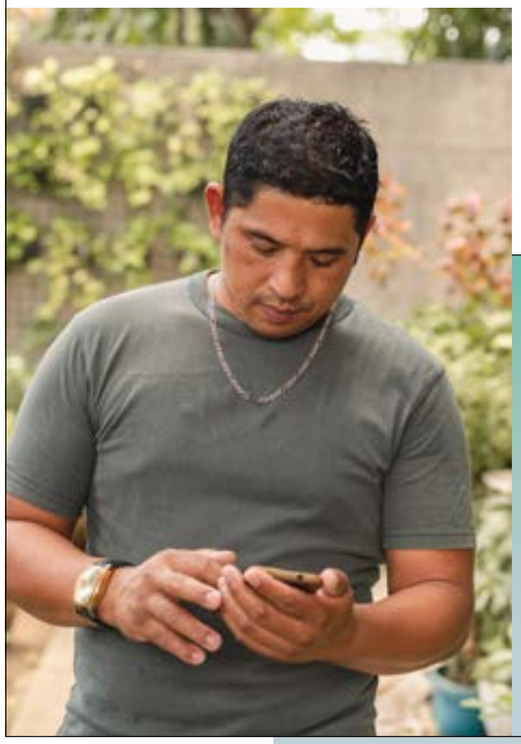
A consumer threat model aims to identify and evaluate potential cybersecurity risks by analyzing likely methods attackers might use in a given scenario. The rise of various piracy services has changed and heightened the risk landscape for individuals, their workplaces, and government entities.

Threat models typically comprise

- (a) a description of the various threat actors
- (b) an analysis of attack vectors
- (c) an impact analysis
- (d) mitigation strategies[31]

Threat actors involved in digital piracy-related cybersecurity threats include cybercriminals who exploit vulnerabilities in piracy platforms for financial gain or malicious activities, such as spreading malware or stealing data. Hacktivists may target these platforms to support or disrupt access to pirated content for ideological reasons. State-sponsored actors may engage in cyber espionage, often for intelligence gathering or political objectives.

Additionally, inexperienced hackers, often referred to as “script kiddies,” may exploit these platforms using pre-made tools, contributing to the overall threat landscape. Out of these alternatives, previous research has indicated a strong link between organized crime and digital piracy[32].



Some of the main attack vectors are further described in the following sections.

ILLICIT STREAMING SERVICES

Unauthorized streaming provides instant access to content without requiring full file downloads, typically through subscription or advertisement-supported models, noting that advertising can also be used to deliver malware[33]. These illicit platforms often feature live channels for movies, TV shows, and sports events, sometimes including on-demand video options. Users may pay a single fee to access multiple premium services, but the original content creators and rights holders do not receive this revenue.

These illegal streaming services frequently rely on advertising income, potentially exposing viewers to harmful advertisements or pop-ups that may contain malicious software or deceptive links. Some platforms falsely advertise free access to premium content, deceiving users into providing personal or financial information for purported subscriptions, which can lead to fraudulent activities and identity theft[34].

P2P (PEER-TO-PEER) NETWORKS

Peer-to-peer (P2P) networks enable direct file sharing between users, creating a decentralized system for content exchange. This allows individuals to both upload and download files directly from other participants’ devices. However, these networks can sometimes harbor security risks. Shared files may contain concealed malicious software, potentially compromising users’ devices and exposing personal information. Additionally, these networks may facilitate the spread of deceptive or harmful advertising, as shown in Figure 1.

Figure 1 – Traditional Piracy Threat Model

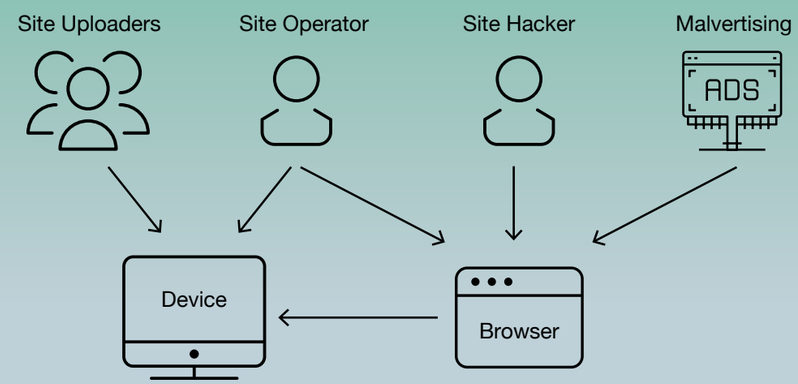
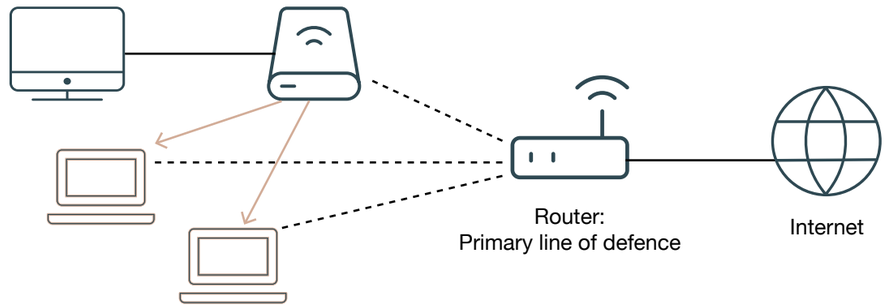


Figure 2 – Threat Model – IPTV Subscription Services



PROXY SERVICES

Proxy services are often used in digital piracy to bypass geographical restrictions, enabling users to access content that would otherwise be blocked in their region – typically as a result of judicial or regulatory site blocking. By routing internet traffic through these proxy servers, users can mask their real IP addresses, making it difficult for authorities to trace their online activities, and facilitating the bypass of website blocking. These proxies can be free or paid, with some specifically marketed for accessing illegal streaming sites, P2P networks, or other pirated content. However, using these services exposes users to significant risks, as many proxy sites may inject malware, track user activity, or operate as scams to harvest personal data[35]. Additionally, they might downgrade secure connections, leading to potential data interception and identity theft.

IPTV SUBSCRIPTION PIRACY SERVICES

IPTV Subscription Piracy Services[36] offer access to a range of content, including live channels for films, TV shows, and sports events, often alongside video-on-demand options. Video on Demand (VOD) features are often included in these illicit IPTV packages, allowing users to access a library of movies and TV shows at their convenience.

This on-demand content complements the live streaming options, providing a more comprehensive entertainment package that mimics legitimate streaming services, but without proper licensing or compensation to content creators and rightsholders. Users typically pay a single fee for access to multiple premium services, but this revenue doesn't reach the legitimate content owners. These illicit services usually require payment, putting users at risk of financial loss. Subscribers may need to provide sensitive financial information, potentially exposing themselves to payment fraud or unauthorized access to their accounts.

A recent study by the Digital Citizens Alliance[37] highlighted these risks. The threat model is summarized in Figure 2.

FRAUDULENT PIRACY SITES

Fraudulent piracy websites masquerade as piracy platforms to swindle users. These sites often mimic the layout, advertising style, and even domain names of popular unauthorized content sharing platforms. However, users soon discover they cannot access the promised pirated content, as the true intention is to steal personal information or financial details[38].

These fraudulent sites do not actually host any content. Instead, they may lure users into purchasing expensive subscriptions after obtaining credit card information. Some trick users into divulging personal data, potentially leading to identity theft or phishing attacks where cybercriminals exploit the collected information.

Users may be duped into paying for access to non-existent content or services, resulting in financial losses without receiving the advertised material. The end goal of these sites is often to acquire sensitive data or money through deception, rather than to provide any actual content, pirated or otherwise.

An evolving threat model for digital piracy

The digital landscape's evolution, driven by technological advancements and changing user behaviors, necessitates a sophisticated understanding of new risks.

Illicit content often serves as a vector for malware distribution, potentially compromising users' devices and personal data. Malware techniques are becoming increasingly complex, with methods like polymorphic malware challenging traditional security measures. Users may fall prey to fraudulent subscription services, losing money, or exposing financial information to illegitimate platforms. Scammers are adopting more sophisticated tactics, closely mimicking legitimate services, making it challenging for users to discern authentic from fraudulent offerings.

Unauthorized streaming services have been known to mishandle user data, leading to privacy violations. With more advanced tracking technologies emerging, the scope of potential privacy breaches has expanded, potentially involving more detailed user profiling and data exploitation.

The unlawful distribution of copyrighted content can have broader economic impacts, but also specific risks for consumers.

Across illicit services, users providing personal information risk privacy breaches, with data potentially being collected and misused without consent. Unauthorized platforms and fraudulent sites may also be involved in data breaches, exposing sensitive information like financial details and passwords to potential exploitation.

What is the financial situation of consumers in the Philippines?

The Philippine economy has been on a steady growth trajectory, largely driven by robust domestic demand, and a thriving services sector, particularly in Business Process Outsourcing (BPO). However, the economy has also faced periods of fluctuating inflation, which has at times impacted the purchasing power of consumers. When inflation rates rise, the costs of basic goods and services increase, leading to financial strain on households that already operate on tight budgets.

Income levels in the Philippines vary significantly, between metropolitan and regional areas, sometimes not meeting the true cost of living, which exacerbates financial pressures on lower-income households. Many families receive some level of support from extended family living overseas, or from their communities, being strongly rooted in mutual support and assistance concepts such as bayanihan, utang na loob and kapitbahay.

Debt plays a substantial role in the financial lives of many Filipinos, who often resort to personal loans, credit card debt, and informal lending practices, to meet their needs. Offsetting this has been a 5.6 percent year-on-year gain in GDP, driven by a strong services industry[39].

Financial inclusion has been improving in the Philippines, with advancements in mobile banking and fintech solutions making financial services more accessible, especially in rural areas. However, a significant portion of the population remains unbanked or underbanked, limiting their access to credit and formal financial services. This challenge is particularly acute for those without formal employment or sufficient collateral.

In terms of consumer behavior, Filipinos typically prioritize spending on essentials like food, housing, and education. Discretionary spending is more common among middle to upper-income groups, who have greater financial flexibility. The COVID-19 pandemic has further influenced consumer habits, leading many to adopt a more cautious approach, focusing on saving and minimizing unnecessary expenses.

Optimism appears to be high across households[40]. Despite these improvements, challenges persist. The rising cost of living, especially in urban areas, continues to put pressure on household finances. Additionally, the informal economy remains a significant part of the Philippine labor market, where workers may lack access to social security benefits and health insurance, further contributing to their financial vulnerability.

In summary, it is easy to understand why some Filipino consumers may be lured by the promise of “free” or cheaper digital content being offered by piracy services but may be unaware of the cybersecurity risks involved.

Why are Filipino consumers attractive targets for cyber threats?

Filipino consumers are particularly attractive targets for cyber threats linked to digital piracy sites due to several factors. First, while discretionary spending remains high[41], the economic challenges in some households make the lure of free or low-cost access to premium content through piracy sites particularly strong. This financial motivation often outweighs concerns about security risks, leading to higher engagement with potentially dangerous platforms.

Additionally, the level of digital literacy varies widely across the population, with many users lacking awareness of the cybersecurity risks associated with these sites, such as malware, phishing, and data theft. The prevalence of mobile device usage in the Philippines, coupled with limited access to robust cybersecurity tools, further exacerbates the vulnerability of consumers. Many users access piracy sites through smartphones, which may not have adequate protection against sophisticated cyber threats. While digital transformation remains a longstanding government priority[42], digital literacy sits behind a number of other comparable ASEAN economies[43].

Furthermore, the high volume of internet usage and social media engagement in the Philippines provides a rich environment for cybercriminals to distribute malicious content or launch targeted attacks[44]. The widespread use of proxies and VPNs to access geo-restricted content can also expose users to man-in-the-middle attacks, where attackers intercept and manipulate communications.

These factors, combined with the growing sophistication of cyber threats, make Filipino consumers prime targets for attacks related to digital piracy. The reliance on digital piracy sites not only puts their personal information and devices at risk but also exposes them to financial fraud, identity theft, and other forms of cybercrime[45].

What are the protective factors in terms of cyber policy and regulatory responses?

Protective factors in terms of cyber policy and regulatory responses for Filipinos concerning digital piracy include several key initiatives and legal frameworks aimed at reducing the risks associated with cyber threats.

1. **IPOPHL's Rules on Voluntary Administrative Site Blocking ("Site Blocking Rules" – Memorandum 23-025)[46]:** An expedited approach to voluntary administrative site blocking for ISPs, including site blocking using DNS, IP addresses, URLs, or any other technical means for preventing access to piracy websites. For piracy sites hosting malware and other cyber threats, these new rules provide a high level of consumer protection. However, the major weakness is the voluntary nature of the control.

2. **Cybercrime Prevention Act of 2012 (Republic Act No. 10175)[47]:** This law is a cornerstone of the Philippines' efforts to combat cybercrime, including those related to digital piracy. It provides a legal basis for prosecuting cybercriminals and offers protection to users by criminalizing a wide range of cyber offenses, such as hacking, identity theft, and the spread of malicious software.

3. **National Cybersecurity Plan 2022[48]:** The Philippines has implemented a comprehensive cybersecurity strategy that emphasizes the protection of critical infrastructure, government, and private sector networks. This plan also promotes awareness and education on cybersecurity among the public, including the risks associated with digital piracy.

4. **Intellectual Property Code of the Philippines (Republic Act No. 8293)[49]:** This law, which has been updated to address the challenges of the digital age, aims to protect intellectual property rights. It includes provisions for combating online piracy, with enforcement mechanisms that target illegal streaming sites, P2P networks, and other platforms that distribute pirated content.

5. **House Bill 7600[50], Senate Bills 2150[51], 2385[52], 2645, and 2651:** Legislative measures aimed at strengthening the country's intellectual property protections, moving beyond the voluntary site blocking measures described above. The IPOPHL would have greatly expanded powers to block access to piracy sites, and thereby protect consumers from cybersecurity threats operating from those sites.

These protective factors work together to create a safer digital environment for Filipinos by reducing the prevalence of digital piracy and mitigating the associated cybersecurity risks.

While challenges remain, these policies and regulatory responses represent significant steps toward protecting consumers from the dangers linked to illegal online activities. While House Bill 7600 has passed, the Senate Bills are awaiting passage as of October 2024.

SUMMARY OF STUDY AIMS

Considering the consumer threat model, economic factors, cybersecurity risks, and legislative protections, a key missing element in the broader debate is being able to quantify the cybersecurity risks for Filipino consumers from accessing piracy sites. Using a methodology that has been peer reviewed and utilized across a range of countries, this report presents the findings of a cyber risk quantification study that seeks to answer the research question – are Filipinos exposed to greater cybersecurity risk from visiting piracy sites, when compared to popular mainstream sites, and if so, how much greater is the risk?

Methods

02

Methods

This study used data relating to the Philippines to evaluate cyber risks linked to piracy websites. The assessment utilized VirusTotal, a Google-owned tool that scans websites for various threats including malware, phishing, and spam content.

VirusTotal's effectiveness stems from its ability to cross-reference data from over 90 antivirus vendors and execute potentially harmful code in a controlled environment. This tool played a crucial role in establishing risk metrics, including threat encounter probabilities, which were compared against the most popular mainstream sites for Filipinos.

The Alliance for Creativity and Entertainment (ACE)[53] provided a list of piracy and fraudulent websites popular in the Philippines, offering unauthorized film and TV content. ACE compiled this list using data from copyright removal requests, site blocks in various countries, and other credible sources. Specific samples were selected from this list for analysis.

To ensure a valid comparison, a control sample consisting of the 30 most popular legal film/TV sites in the Philippines was also evaluated, using data from SimilarWeb from May 2024. Each sample group contained 30 sites, allowing for reliable population inferences using sample standard deviation to calculate standard error. This methodology ensured representative samples and an experimental design with proper controls.

Data samples representing specific categories were analyzed during August 2024 based on consumer website visits in the Philippines.

These samples were organized as follows:

- The top 30 IPTV Subscription Service sites
- The top 30 streaming piracy sites
- The top 30 P2P piracy sites
- The top 30 proxy sites
- The top 30 fraudulent piracy sites

During the study period, the "Top 30" designation referred to the most frequently visited sites in the designated category. This approach aligns with the Pareto Principle, which suggests that a small number of sites likely account for the majority of user traffic[54].

It's important to note that the fraudulent piracy sites, as independently verified by ACE, did not actually host any pirated content. This distinction between genuine piracy sites and fraudulent ones was deemed crucial for the study. These fraudulent sites operate by deceiving users into purchasing expensive subscriptions after obtaining their credit card information, rather than providing any actual content. While all unauthorized content sites carry inherent risks, the expectation was that these fraudulent platforms may present an even higher level of danger due to their intentionally deceptive nature.

Results

03

Worst Case and Best Case Likelihood Scenarios
IPTV Client Software Analysis

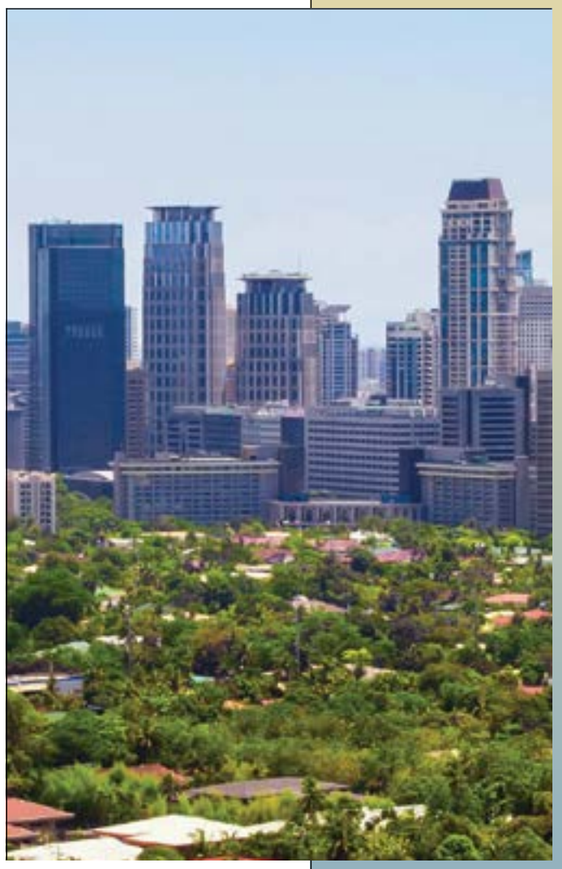
Results

The study analyzed 180 website URLs across six categories: IPTV Subscription Services, Top 30 Streaming, Top 30 P2P, Top 30 Proxy, Top 30 Fraudulent, and Control. These were submitted to VirusTotal[55] for evaluation.

The results were systematically organized into six cyber risk categories:

1. **Malicious:** Sites confirmed by human assessment to contain cyber threats.
2. **Suspicious:** Sites flagged by machine detection as potentially harboring cyber threats.
3. **Malware:** Sites distributing malicious software.
4. **Phishing:** Sites designed to illicitly obtain user credentials.
5. **Spam:** Sites used for unsolicited emails, pop-ups, or automated commenting.
6. **Not Recommended:** Sites potentially distributing unwanted software.

These classifications are based on reports from over 90 partners, including major cybersecurity threat detection companies. This collaborative effort aims to identify websites actively involved in cyber threat dissemination. Each detection company reports only one category per site, reflecting their assessment of the site's primary risk.



Worst Case and Best Case Likelihood Scenarios

In our analysis, we provide both worst-case and best-case likelihood estimates based on independent reports from various antivirus vendors on VirusTotal. Since each vendor uses different definitions and maintains proprietary threat databases, the best-case estimate conservatively assumes that all vendors are detecting the same malware sample. In contrast, the worst-case estimate assumes that each detection is of a different sample. Although most detections appear to be distinct, we present this range for clarity.

Tables 1 and 2 show the worst-case and best-case scenarios for P2P, streaming, fraudulent sites, and a control group in the Philippines[56]. The worst-case scenario estimates suggest that the likelihood of encountering a cyber threat is 2.20 on Top 30 P2P sites, 2.13 on Top 30 streaming sites, 1.07 on IPTV sites, 1.90 on Top 30 proxy sites, and 2.00 on Top 30 fraudulent sites, with control sites showing a likelihood of 0.13. In the best-case scenario, P2P sites have a likelihood of 1.43, streaming sites 1.27, IPTV sites 0.67, proxy sites 1.03, and fraudulent sites 1.03, with control results remaining consistent in both cases.

In simpler terms, when the likelihood is greater than one, it means consumers are likely to encounter at least one cyber threat. By comparing these findings to a control group of the most popular 30 legal film/TV sites in the Philippines, we can see just how elevated this risk is.

For instance, a likelihood of 2.20 means that for every piracy site visited, a consumer is exposed to an average of 2.20 cyber threats, which is very high. Essentially, each visit to a piracy site exposes users to multiple threats – a pattern consistent across all types of site.

Regarding IPTV, this analysis only examined the landing pages of IPTV subscription services, not the service itself, as malware could also be present in the software used for these platforms. Previous research has indicated that the software used in IPTV set-top boxes is often pre-loaded with malware in multiple markets, including Europe[57], the United States[58] and Singapore[59]. It is possible that once consumers pass through the landing page into a subscription environment, the specific risks may be different, or more or less frequent.

In summary, if the likelihood is above one, consumers are expected to encounter at least one cyber threat on average. To quantify how much greater this risk is compared to normal browsing, we used a control group of the most popular 30 legal film/TV sites in the Philippines. Table 3 shows that the relative risk of encountering a cyber threat is 33.00 times higher for P2P sites, 32.00 times higher for streaming sites, 30.00 times higher for fraudulent sites, 28.50 times higher for proxy sites, and 16.00 times higher for IPTV sites. This means that using piracy sites or services in the Philippines exposes consumers to significantly higher risks of cyber threats.

Table 1 – Worst-case scenario - Average likelihood of all cyber threats

Illegal IPTV

Country	N	Detections	Likelihood
Philippines	30	32	1.07

Streaming

Country	N	Detections	Likelihood
Philippines	30	64	2.13

P2P

Country	N	Detections	Likelihood
Philippines	30	66	2.20

Proxy

Country	N	Detections	Likelihood
Philippines	30	57	1.90

Fraudulent

Country	N	Detections	Likelihood
Philippines	30	60	2.00

Control

Country	N	Detections	Likelihood
Philippines	30	2	0.07

Table 2 – Best-case scenario - Average likelihood of all cyber threats

Illegal IPTV

Country	N	Detections	Likelihood
Philippines	30	20	0.67

Streaming

Country	N	Detections	Likelihood
Philippines	30	38	1.27

P2P

Country	N	Detections	Likelihood
Philippines	30	43	1.43

Proxy

Country	N	Detections	Likelihood
Philippines	30	31	1.03

Fraudulent

Country	N	Detections	Likelihood
Philippines	30	31	1.03

Control

Country	N	Detections	Likelihood
Philippines	30	2	0.07

Table 3 - Relative Risk Calculation

Worst Case Scenario

Country	Illegal IPTV	Streaming	P2P	Proxy	Fraud	Average
Philippines	16.00	32.00	33.00	28.50	30.00	27.90

Best Case Scenario

Country	Illegal IPTV	Streaming	P2P	Proxy	Fraud	Average
Philippines	10.00	19.00	21.50	15.50	15.50	16.30

Discussion

04

What regulatory reforms could reduce cyber risk?

How could law enforcement be better resourced?

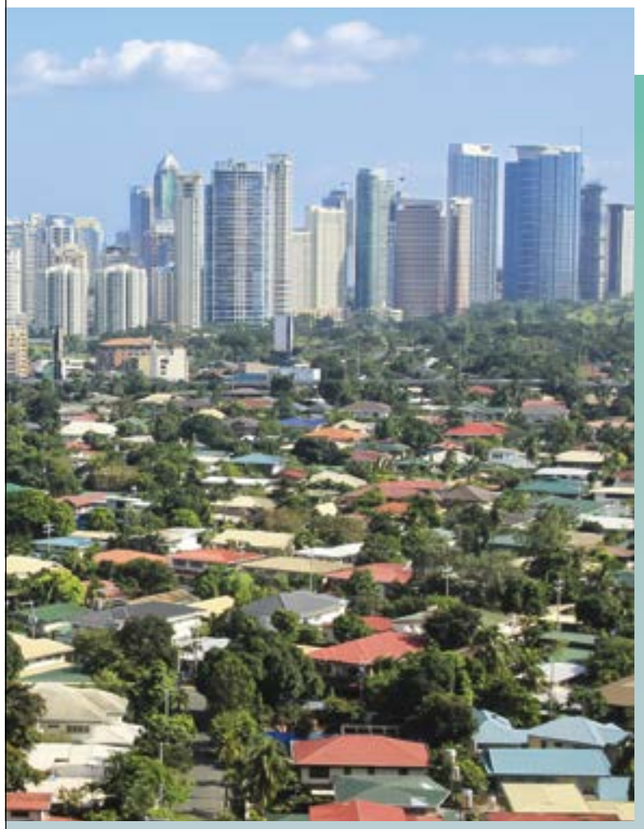
How could consumer awareness and education reduce cyber risk in relation to piracy sites?

Discussion

The findings of this study reveal a significantly high risk of encountering cyber threats when using digital piracy services in the Philippines.

In the worst case scenario, a consumer visiting the Top 30 P2P piracy sites would face exposure to 66 cyber threats in total, with a relative risk of 33.00 compared to mainstream websites. Similar rates were observed for Streaming sites (66 threats, relative risk of 32.00), and scam sites (60 threats, relative risk of 30.00). By assessing this relative risk against a baseline level of cyber risk from visiting any website, we can quantify the increased danger associated with accessing digital piracy sites. Implementing faster and more comprehensive blocking of these sites could lead to a substantial reduction in overall cyber risk in the Philippines, especially given the already elevated threat levels, as per SB 2385, SB 2150 and HB 7600.

We offer several policy recommendations for Filipino authorities to consider in their efforts to further reduce cyber risks for consumers, particularly for the many who are likely to be teenagers or younger. Based on the evidence in this report, the most crucial reform would be to introduce administrative site blocking, allowing for the transparent and timely blocking of a select number of high-risk websites.



Summary

Filipino consumers are at very heightened cybersecurity risk when they visit piracy sites. These sites also damage the Filipino creative sector. Legislative change is underway that, in combination with existing voluntary measures and cybersecurity strategies, will further protect Filipino consumers, and lay the foundations for economic growth arising from an environment in which cybercriminals are prevented from making illicit gains by stealing the identities of those consumers.

What regulatory reforms could reduce cyber risk?

Given the urgency of “zero day” cyber threats, timely and proportionate actions are essential to mitigate the risks to consumers from infections or exploitation. This underscores the importance of passing Senate Bills 2150 and 2385, as their provisions for rapid compliance with directives from IPOPHL will help minimize the impact of zero-day attacks on consumers. In summary, the Philippines should move from the current voluntary scheme to a mandatory, rapid scheme, with appropriate checks and balances to prevent overblocking.

Reducing cyber risks in the Philippines, particularly those arising from digital piracy requires a multifaceted approach combining regulatory reforms, collaboration, and technological advancements. Refining national regulations to align with global standards could strengthen the country’s overall cybersecurity stance, while specifically addressing increased risks due to piracy. Additional national cybersecurity planning could address emerging threats, clearly define responsibilities, and establish measures for protecting critical infrastructure and sensitive data that may be affected by proxies and VPNs that could introduce threats behind corporate or government firewalls. Further developing voluntary data breach notification requirements would promote prompt incident reporting, allowing for faster response and mitigation efforts, especially where these are piracy-related.

Enforcing cybersecurity standards across critical infrastructure sectors and encouraging organizations to obtain cybersecurity certifications that reflect industry best practices can also help reduce sector-wide cyber risks arising from piracy. Organizations should be mandated to develop and regularly test incident response plans to ensure they are prepared to respond swiftly to cyber incidents originating from consumers visiting piracy sites. Additionally, addressing supply chain security through regulation, by requiring organizations to assess and manage the cybersecurity risks associated with their suppliers and service providers, is crucial. Organizations should be encouraged to evaluate and monitor the cybersecurity practices of their vendors and partners to further safeguard their operations, with specific guidance provided in relation to malware threats arising from piracy.

How could law enforcement be better resourced?

Addressing cyber threats from piracy sites in the Philippines requires a comprehensive approach that integrates legal, technological, and collaborative efforts to ensure that law enforcement is well-equipped. Establishing specialized cybercrime units within law enforcement agencies, focused on combating online piracy and related threats, is essential.

These units should be provided with advanced training in digital forensics, cybersecurity, and intellectual property enforcement. Additionally, ongoing capacity building and training programs are crucial, as cyber threats constantly evolve. Law enforcement personnel must stay updated on the latest trends, investigative techniques, and digital tools to respond effectively[60].

Investing in the necessary technological infrastructure is also vital for enabling law enforcement agencies to conduct thorough digital investigations and respond to cyber threats. This includes access to tools for digital forensics, data analysis, and collaboration platforms. Enhancing the capability to handle digital evidence, ensuring its admissibility in court, and training law enforcement officers in preserving and presenting this evidence during legal proceedings are critical components of this effort.

Supporting victims of cybercrime through strengthened mechanisms and establishing user-friendly reporting systems can also expedite the investigation and response to cyber threats. Encouraging prompt incident reporting from individuals and businesses will enhance law enforcement's ability to take swift action. An innovative approach could involve implementing a one-click reporting tool that allows consumers to flag cyber threats encountered on piracy sites, capturing crucial digital evidence and preserving it for enforcement action. For such innovations to be effective, incident response and triage systems must be in place, along with administrative site blocking to quickly mitigate identified threats.

By integrating these strategies, the Philippines can better prepare its law enforcement agencies to tackle the cyber threats posed by piracy sites.

How could consumer awareness and education reduce cyber risk in relation to piracy sites?

Raising consumer awareness and education is crucial in mitigating the cyber risks associated with piracy sites in the Philippines. By educating consumers, particularly teens and pre-teens, about the dangers of engaging with piracy sites and encouraging responsible online behavior, they can make more informed choices. While noting the important emphasis on effective cybercrime prevention through the Cybercrime Prevention Act (2012)[61], an effective action plan specifically related to consumer education should include the following strategies:

- Inform consumers about the various risks linked to piracy sites, including exposure to malware and phishing attacks. The information should stress the dangers of downloading or streaming content from unauthorized sources, and train people how to identify legitimate sources.
- Highlight the increased risk of malware infections and other cyber threats that piracy sites pose. Consumers need to understand that these sites often harbor malicious software, putting their devices at risk of ransomware, identity theft, credit theft, spyware, and sextortion.
- Raise awareness about phishing tactics frequently used by cybercriminals on piracy sites. Consumers should be vigilant about sharing personal information, such as login credentials or financial details, on suspicious websites. Consideration should be given to population-wide training on how to spot phishing sites, especially as several piracy sites in this study were identified as also operating as phishing sites.
- Provide guidance on safe online practices, such as the importance of keeping software and antivirus programs up to date, and the dangers linked to piracy sites and services.
- Promote the use of legitimate streaming services and official content distribution platforms to reduce exposure to cyber threats.
- Incorporate digital literacy programs into educational curricula and public awareness campaigns. Equip individuals with the skills and knowledge needed to safely navigate the digital landscape, identify potential threats, and make informed decisions. The Philippines ranks comparatively low on privacy awareness skills compared to other ASEAN nations[62].
- Launch public awareness campaigns to educate consumers about the risks associated with piracy sites. Utilize various channels, including social media, educational institutions, and government initiatives, to spread information and encourage responsible online behavior.
- Work with Internet Service Providers (ISPs) who can help educate their subscribers about the associated risks.
- Integrate cybersecurity concepts into media literacy programs to help individuals critically evaluate online content sources and understand the potential risks of consuming content from unverified platforms.

Implementing these strategies aligns with the broader objectives outlined in the National Cybersecurity Plan 2022, and further protects consumers.

Bibliography

05

Bibliography

Bibliography

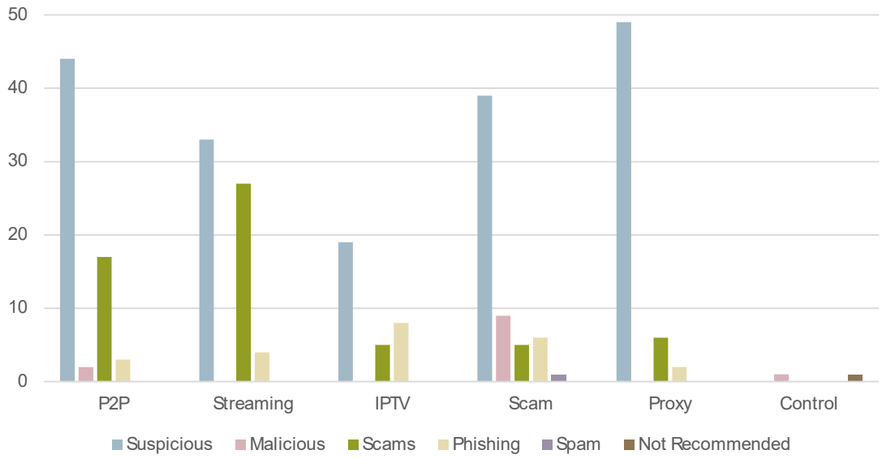
1. https://ipkey.eu/sites/default/files/ipkey-docs/2023/IPKeySEA_November2023_Atty-Christine-Canlapan_Updates-on-the-National-Legislation-and-Initiatives-on-Copyright-Protection.pdf
2. https://www.globe.com.ph/about-us/newsroom/corporate/online-piracy-ph-reaches-70-percent#gref
3. https://www.lightreading.com/digital-transformation/philippines-approves-288m-digital-infrastructure-project
4. Stokes, N. (2024). Strategies to Reduce the Impact of Digital Piracy in the Media Industry. Doctoral thesis – Walden University (https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=16875&context=dissertations)
5. Rajavi, K., Danaher, B., & Newby, J. (2024). Price, Piracy, and Search: Which Pirates Respond to Changes in the Legal Price?. MIS Quarterly.
6. Iqbal, A., Aman, M. N., Rejendran, R., & Sikdar, B. (2024). Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study. IEEE Open Journal of the Computer Society.
7. Watters, P., Mantri, S., & Gangwar, M. (2024). The Piracy-Malware Nexus in India: A Perceptions and Experience and Empirical Analysis. Available at SSRN 4766797.
8. Reis, F., de Matos, M. G., & Ferreira, P. (2024). Controlling digital piracy via domain name system blocks: A natural experiment. Journal of Economic Behavior & Organization, 218, 89-103.
9. Danaher, B., Smith, M. D., & Telang, R. (2014). Piracy and copyright enforcement mechanisms. Innovation policy and the economy, 14(1), 25-61.
10. As per [1], Media Partners Asia estimates $1b revenue leakage in the Philippines by 2027, and losses of $781m in 2022.
11. Kumar, S., Madhavan, L., Nagappan, M., & Sikdar, B. (2016). Malware in pirated software: Case study of malware encounters in personal computers. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 423-427).
12. Watters, P. (2021). Consumer Risk and Digital Piracy–Where Does Malware Come From?. Available at SSRN 4536938.
13. Watters, P. A., & McCombie, S. (2011). A methodology for analyzing the credential marketplace. Journal of Money Laundering Control, 14(1), 32-43.
14. McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys (CSUR), 54(9), 1-36.
15. https://www.pids.gov.ph/publication/policy-notes/why-literacy-measurement-deserves-rethinking
16. https://eprajournals.com/IJMR/article/12214/download
17. https://www.globe.com.ph/about-us/newsroom/corporate/online-piracy-ph-reaches-70-percent#gref
18. https://www.zawya.com/en/world/china-and-asia-pacific/online-site-blocking-bill-pushed-to-curb-digital-piracy-in-philippines-hnhf4stx
19. Moreno, N. I. S., & Quimba, F. M. A. (2022). Assessing Policy Impacts in Digital Services Trade: Implications for the Philippines (No. 2022-29). PIDS Discussion Paper Series.
20. SMITH, M. D. (2023). What the Online Piracy Data Tells Us About Copyright Policymaking. Hudson Institute Policy Memo.
21. Danaher, B., Smith, M. D., & Telang, R. (2020). Piracy landscape study: Analysis of existing and emerging research relevant to intellectual property rights (IPR) enforcement of commercial-scale piracy. USPTO Economic Working Paper No. 2020-02.
22. Scaraboto, D., Almeida, S. O. D., & dos Santos Fleck, J. P. (2020). “No piracy talk”: how online brand communities work to denormalize controversial gaming practices. Internet Research, 30(4), 1103-1122.
23. Fink, C., Maskus, K. E., & Qian, Y. (2016). The economic effects of counterfeiting and piracy: A review and implications for developing countries. The World Bank Research Observer, 31(1), 1-28.
24. Liu, L., Zhang, W., & Han, C. (2021). A survey for the application of blockchain technology in the media. Peer-to-Peer Networking and Applications, 14(5), 3143-3165.
25. Telang, R. (2018). Does online piracy make computers insecure? evidence from panel data. Evidence from Panel Data (March 12, 2018).
26. Watters, P. (2021). Consumer Risk and Digital Piracy–Where Does Malware Come From?. Available at SSRN 4536938.
27. https://cybernews.com/security/zlibrary-copycat-exposes-millions-digital-pirates/
28. Jakobi, A. P. (2020). Crime, Security and Global Politics: An Introduction to Global Crime Governance. Bloomsbury Publishing.
29. Kruessmann, T. (2022). Organized Crime. In International Conflict and Security Law: A Research Handbook (pp. 1207-1226). The Hague: TMC Asser Press.
30. Watters, P. A. (2018). Investigating malware epidemiology and child exploitation using algorithmic ethnography. In 51st Annual Hawaii International Conference on System Sciences, HICSS 2018 (pp. 5284-5293). Institute of Electrical and Electronics Engineers (IEEE).
31. Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 231-271). Cham: Springer Nature Switzerland.
32. https://rouse.com/insights/news/2024/enforcement-amid-digital-piracy-and-organized-crime-in-vietnam
33. Watters, P. (2013). A systematic approach to measuring advertising transparency online: An Australian case study. Available at SSRN 2362621.
34. Watters, P. A., Watters, M. F., & Ziegler, J. (2015). Maximising eyeballs but facilitating cybercrime? ethical challenges for online advertising in new zealand. In 2015 48th Hawaii International Conference on System Sciences (pp. 1742-1749). IEEE.
35. https://www.linkedin.com/pulse/malware-turned-thousands-hacked-windows-macos-pcs-proxy-ahmed-osama/
36. Rajiv Shah, Deniz Cemiloglu, Cagatay Yucel et al. Is cyber hygiene a remedy to IPTV infringement? A study of online streaming behaviours and cybersecurity practices, 12 November 2023, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-3579394/v1]
37. https://www.digitalcitizensalliance.org/news/press-releases-2023/piracy-subscription-services-drive-credit-card-fraud-and-other-harms-to-consumers-new-digital-citizens-alliance-investigation-and-survey-finds/
38. Iqbal, A., Aman, M. N., Rejendran, R., & Sikdar, B. (2024). Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study. IEEE Open Journal of the Computer Society.
39. https://think.ing.com/articles/philippines-consumers-take-on-more-debt-save-less/
40. https://www.transunion.ph/content/dam/transunion/ph/business/collateral/report/philippines-consumer-pulse-report-q4-2023.pdf
41. https://www.manilatimes.net/2023/12/19/business/top-business/discretionary-spending-expected-to-rise-in-2024/1924838
42. Treceñe, J. K. D. (2021). The digital transformation strategies of the Philippines from 1992 to 2022: A review. Eng. Technol. Rev, 2, 8-13.
43. Kusumastuti, A., & Nuryani, A. (2020, March). Digital literacy levels in ASEAN (comparative study on ASEAN countries). In IISS 2019: Proceedings of the 13th International Interdisciplinary Studies Seminar, IISS 2019, 30-31 October 2019, Malang, Indonesia (p. 269). European Alliance for Innovation.
44. Blancaflor, E., Dela Cruz, R. G., Federez, U. A., & Samonte, D. (2023). Social Media Content Compilation of Online Banking Scams in the Philippines: A Literature Review. In Proceedings of the 2023 14th International Conference on E-Education, E-Business, E-Management and E-Learning (pp. 236-242).
45. Blancaflor, E. B., Daluz, J. L. C., Garcia, R. A. G., Monton, N. G. S., & Vergara, J. M. S. (2023). A Literature Review on the Pervasiveness of Ransomware Threats and Attacks in the Philippines. Journal of Advances in Information Technology, 14(4).
46. https://www.ipophil.gov.ph/news/ipophl-rolls-out-new-site-blocking-rules-to-stamp-out-piracy-redirect-consumers-to-legit-markets/
47. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
48. https://dict.gov.ph/wp-content/uploads/2017/04/NCSP2022.pdf
49. https://lawphil.net/statutes/repacts/ra1997/ra_8293_1997.html#:~:text=It%20shall%20protect%20and%20secure,property%20bears%20a%20social%20function.
50. https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=HBN-7600
51. https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-2150
52. https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-2385
53. The Alliance for Creativity and Entertainment (ACE) is the world’s leading coalition dedicated to protecting the legal creative market and reducing digital piracy. Driven by a comprehensive approach to addressing piracy through criminal referrals, civil litigation, and cease-and-desist operations, ACE has achieved many successful global enforcement actions against illegal streaming services and unauthorized content sources and their operators. Drawing upon the collective expertise and resources of more than 55 media and entertainment companies around the world—including sports channels and associations—and reinforced by the Motion Picture Association’s content protection operations, ACE protects the creativity and innovation that drives the global growth of core copyright and entertainment industries. For more information, visit www.alliance4creativity.com
54. The top 30 sites in these categories average 80% of the total category visits from the Philippines.
55. For more details of how VirusTotal works, see https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
56. The control group in this study consisted of the most popular legal film/TV websites in the Philippines. In contrast, prior studies utilized a control group comprising the most popular websites overall. The current control group offers a more appropriate comparison, as it ensures a closer match between the control and experimental groups, thereby enhancing the validity of the matched samples approach.
57. Watters, P.A (2021), Time to Compromise: How Cyber Criminals use Ads to Compromise Devices through Piracy Websites and Apps. Available at SSRN: https://ssrn.com/abstract=4536943
58. Lockett A, Chalkias I, Yucel C, Henriksen-Bulmer J, Katos V. Investigating IPTV Malware in the Wild. Future Internet. 2023; 15(10):325. https://doi.org/10.3390/fi15100325
59. Watters, P.A (2024), Scams, Cyber Threats and Illicit Sports Streaming in Singapore. Available at SSRN: https://ssrn.com/abstract=4709637
60. https://cybercrime.doj.gov.ph/
61. https://legalresearchph.com/2021/12/05/r-a-no-10175-the-cybercrime-prevention-act-the-net-commandments/
62. https://btf.rappler.com/257/asean-foundation-unveils-research-findings-on-digital-literacy-spotighting-the-digital-divide-across-the-region/

Appendices

Appendix A

Cyber threat category results – Worst-case scenario

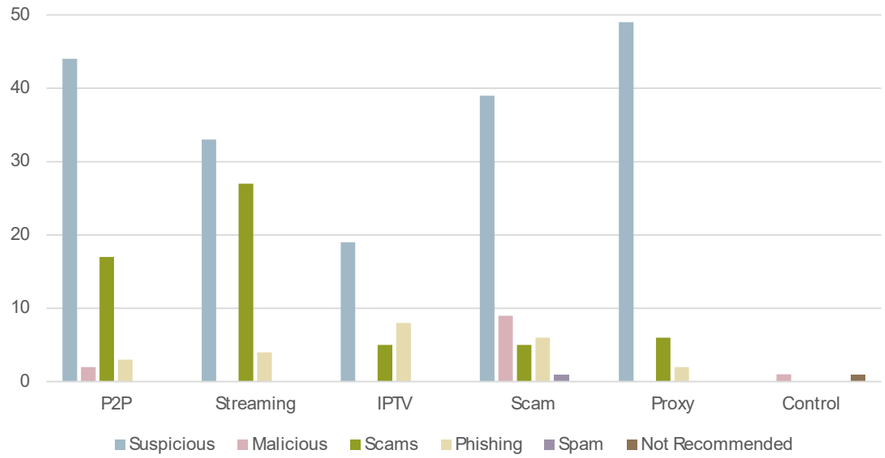
	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
P2P	44	2	17	3	**0**	**0**
Streaming	33	0	27	4	**0**	**0**
IPTV	19	0	5	8	**0**	**0**
Scam	39	9	5	6	**1**	**0**
Proxy	49	0	6	2	**0**	**0**
Control	0	1	0	0	**0**	**1**



Appendix B

Cyber threat category results – Best-case scenario

	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
P2P	26	2	12	3	**0**	**0**
Streaming	17	0	17	4	**0**	**0**
IPTV	12	0	5	3	**0**	**0**
Scam	18	4	4	4	**1**	**0**
Proxy	23	0	6	2	**0**	**0**
Control	0	1	0	0	**0**	**1**



Notes

Researcher Biography

Professor Watters is a trusted cybersecurity researcher and thought leader at Cyberstronomy Pty Ltd. He is the author of *Counterintelligence in a Cyber World* (Springer - ISBN 978-3031352867) and *Cybercrime and Cybersecurity* (CRC Press - ISBN 978-1032524511). Professor Watters is Honorary Professor of Security Studies and Criminology at Macquarie University, and Professor of Information Systems at Holmesglen Institute. Professor Watters is a Chartered IT Professional, a Fellow of the British Computer Society, a Senior Member of the IEEE, Member of the ACM, and a Member of the Australian Psychological Society. His work has been cited 9,176 times, with a *h*-index of 43, and an *i*-10 index of 139. He is in the Top 10% of SSRN-cited authors globally and ranked within the top 0.84% of researchers worldwide (all fields) by ScholarGPS.

Acknowledgements

Funding for this research was provided by the Motion Picture Association. The work was produced independently by Dr Paul Watters, Macquarie University (Sydney).