Drawn to Cybercrime: Protecting against Online Phishing Scams

Authors
Sam Ault, MSc (Royal Holloway, 2022)
Konstaninos Mersinas, ISG, Royal Holloway

Abstract

Financially motivated cybercrime is shifting from the shadows of the dark web and now finds a welcoming audience on social media and instant messaging applications. In the same way that we see a rise in social media influencers, we now see cyber scam influencers rapidly gaining followers and reputation, generating income from their channels. They do so by promoting scamming activities and services through social media channels that can attract and draw young people to cybercrime. UK cyber scam language emerges as part of a new generational subculture, where easy money is made online and from the safety of the home. Instant messaging applications offer strong encryption and embolden fraudsters to broadcast their scam marketplace messages through various public and private channels, enticing new participants to commit crimes online. These cybercrimes are often highly anonymous and non-physical, remaining extremely difficult to prosecute [a]

[a] This article is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

1 Introduction

The COVID-19 pandemic health crisis in 2020 caused major disruption worldwide, creating a unique set of events in our current lifetime. During this period, more and more people spent time at home and increased their time online. Cybercriminals bombarded the public with pandemic-related phishing scams, which led to widespread suffering and loss of personal information. Phishing is a straightforward attack method but remains a persistent threat and targets human weaknesses by using social engineering techniques to convince victims to hand over their personal information.

With many essential services shifting from physical to online, a dependency on digital accounts, emails, messages and remembering numerous passwords has increased. Fraudsters have been capitalising on this acceleration and through the shared experience of the pandemic, they have become psychological experts, increasingly adopting sophisticated ways of stealing our information. As the pandemic era passes and we go back to normal, hidden layers within the online fraud landscape continue to emerge.

2 Online Fraud

Online cybercrime and sophisticated attempts to defraud victims continue to rise, with a recent crime survey[1] estimate of 3.7 million fraud offences occurring in England and Wales in the year ending September 2022. However, there are likely to be many more cases of online fraud that go unreported to the police, skewing official figures and indicators. Victims blame themselves or feel embarrassed or

[1] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2022

confused about how to report fraud. If a victim reaches their bank, long cases and investigations can occur since different agencies investigate these crimes. As a result, the reported crime numbers will be lower than the actual crime survey data shows.

Authorised Push Payment (APP) fraud
A target victim is tricking into approving and sending a payment to an account controlled by a criminal.

In 2021, only 0.8% of police staff in England and Wales were directly focused on economic crime, with one in 1,000 online fraud offences being solved[2]. As more and more criminal opportunities shift online, the cost to the UK economy will continue to rise. With over £600 million stolen by cybercriminals in the first half of 2022[3], the team at UK Finance have warned that the current level of fraud in the UK should now be considered a national security threat. Another significant concern is online fraud that originates from social media. In a recent letter to the Government[4], UK Finance highlighted that 61% of all reported authorised push payment fraud by volume is connected to Meta, the company that owns social media sites Facebook, Facebook Marketplace, Instagram and WhatsApp. With so few online fraud cases being solved or leading to prosecution, authorities and banking institutions must continue to modernise and rethink their approach.

One specific type of online fraud has been on the rise, known as authorised push payment (APP) scams. APP scams often occur when criminals attempt to persuade a victim to take action quickly, and there are many different scenarios where a victim might inadvertently authorise a payment. Some common examples of APP scams are: **Purchase scam** - when a victim pays for fake goods or services, for example, a concert ticket and never receives it. **Investment scam** - a victim is convinced to move their money to an investment fund that does not exist. **Romance scam** - fraudsters use fake profiles on social media or dating websites to target victims and ask them for money. **Impersonation scam** - in this scenario, a fraudster, often claiming to be from the victim's bank, convinces a target to transfer money to an account they control, bypassing all security controls. Unfortunately, impersonation techniques a very deceptive and can leave a victim at a complete loss. Because the victim initiates the payment, often, a bank will be unable to reverse the payment. Banks have now started to show warning messages, which ultimately shift responsibility towards the victim. If the victim has been confused and convinced by a powerful social engineering attack, warnings, messages and prompts are usually ignored.

For social engineering attacks to be truly effective and persuasive, fraudsters often need to build up a complete profile of a target victim. Through analysis of public social instant messaging broadcast channels, where fraudsters trade victim information freely, i.e. open source intelligence (OSINT), it is clear that combined or chained attacks have a very high chance of success when carried out in quick succession.

3 Chained Attacks

Sophisticated attacks often happen through a series of chained attack events. Phishing is the primary attack method that allows fraudsters to collect and steal personal and financial information, building up complete target financial profiles in real time. By following on with a more devastating secondary social engineering attack, based on specific details of the target, victims are being tricked into handing over their online banking details or inadvertently transferring funds to a criminal's account.

These chained attacks are becoming more frequent, partly due to more widely available one-time password (OTP) bot software, which cybercriminals use to make a victim believe a phone call or message is coming from a trusted source. Suppose a victim inadvertently reveals their time-sensitive one-time password authentication codes through these attacks using OTP bot software. In that case,

[2] https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf

[3] https://www.ukfinance.org.uk/news-and-insight/press-release/uk-finance-calls-urgent-action-all-sectors-fraud-continues-threaten

[4] https://on.ft.com/44PHb88

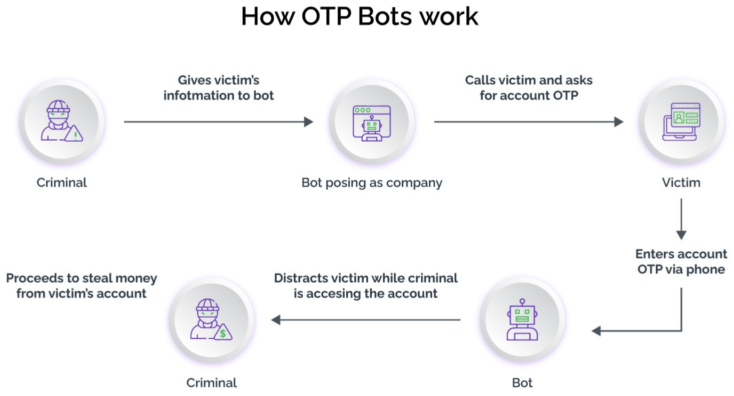

How OTP Bots work
Criminal
Gives victim's infotmation to bot
Bot posing as company
Calls victim and asks for account OTP
Victim
Enters account OTP via phone
Bot
Distracts victim while criminal is accesing the account
Criminal
Proceeds to steal money from victim's account

Figure 1: How OTP bots work, Source: `https://www.arkoselabs.com/explained/otp-bot/`

fraudsters can proceed to take full control of a victim's online bank account.

One-time-password (OTP) bot software is advertised as harmless telephony software. It primarily masquerades as a number-forwarding service, but this software has many hidden malicious features that aid social engineering attacks.

It is not uncommon to find evidence of individuals working together to coordinate and gamify fraudulent activity, which shows the depth of chained attack sophistication. Inside scam instant messaging channels, participants design new phishing approaches together in real-time, discuss tips and tricks and act together as a herd when new victim profile information is shared. Channel subscribers tag and alert each other to highlight new immediately available active victim profiles in an organised manner before performing secondary-stage attacks.

Chained attacks
These types of attacks are more devastating when combined in a rapid attack chain:
1. **Primary attack**: phishing techniques are used to build up complete financial profiles of target victims.
2. **Secondary attack**: an attacker uses social engineering techniques via OTP/spoofing software to masquerade as a financial institution.
The aim is either account takeover (via OTP bot software access) or to get the victim to willingly transfer money to the cybercriminal's account (APP fraud).

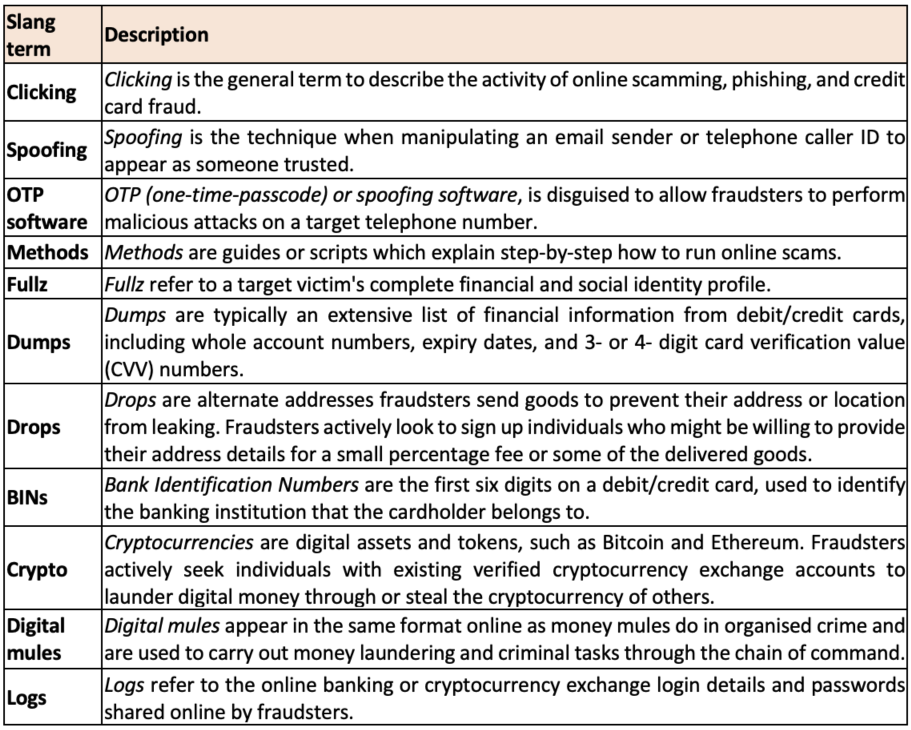
In these these anonymous channel spaces, we see a rise in new slang expressions and various communities beginning to thrive in the excitement of the cyber scam subculture.

4 Cyber Scam Subculture

UK cyber scam subculture and anti-language emerge with new slang expressions and terminology to replace the more traditionally recognised terms, techniques, and elements of online fraud. There appears to be a dangerous growth of socially influenced cybercrime, where scam influencers, just like social media influencers, aim to build followers and increase channel revenue. Fraudsters offer varying tier paid packages through their channels, with various step-by-step guides allowing individuals to commit online fraud easily. These guides provide techniques for UK online retailers, which aim to expose weaknesses in a target system. As online websites try to close loopholes and vulnerabilities, the guide documents are versioned and updated with new techniques and the latest workarounds.

The secrecy of scamming, aided by new slang expressions and anti-language, also leads to a shared sense of belonging for young people who are coerced by the content promoted by these influencers and are welcomed into communities. For some, online scamming might look exciting, and the lure of

Table 1: Common cyber scam anti-language and slang explained.



Slang term	Description
Clicking	*Clicking* is the general term to describe the activity of online scamming, phishing, and credit card fraud.
Spoofing	*Spoofing* is the technique when manipulating an email sender or telephone caller ID to appear as someone trusted.
OTP software	*OTP (one-time-passcode) or spoofing software*, is disguised to allow fraudsters to perform malicious attacks on a target telephone number.
Methods	*Methods* are guides or scripts which explain step-by-step how to run online scams.
Fullz	*Fullz* refer to a target victim's complete financial and social identity profile.
Dumps	*Dumps* are typically an extensive list of financial information from debit/credit cards, including whole account numbers, expiry dates, and 3- or 4- digit card verification value (CVV) numbers.
Drops	*Drops* are alternate addresses fraudsters send goods to prevent their address or location from leaking. Fraudsters actively look to sign up individuals who might be willing to provide their address details for a small percentage fee or some of the delivered goods.
BINs	*Bank Identification Numbers* are the first six digits on a debit/credit card, used to identify the banking institution that the cardholder belongs to.
Crypto	*Cryptocurrencies* are digital assets and tokens, such as Bitcoin and Ethereum. Fraudsters actively seek individuals with existing verified cryptocurrency exchange accounts to launder digital money through or steal the cryptocurrency of others.
Digital mules	*Digital mules* appear in the same format online as money mules do in organised crime and are used to carry out money laundering and criminal tasks through the chain of command.
Logs	*Logs* refer to the online banking or cryptocurrency exchange login details and passwords shared online by fraudsters.

making a lot of money online can be attractive or even a necessity.

Social media fraudsters often have multiple social platforms to help increase their audience. They use instant messaging applications to communicate with their followers and build upon the communities they have created. Telegram is an application that supports public and private broadcast channels, where online scamming products and stolen financial profiles are shared.

5 Anonymous Instant Messaging Channels

Instant messaging applications, such as Telegram and Signal, have increased in popularity due to their privacy-enabling communication features and by offering some of the highest levels of anonymity and encryption. These smartphone applications are easy to use, and with a focus on Telegram, registering a new account only requires a user to enter the most basic information. Telegram has many privacy features, including hiding your telephone number and choosing a pseudonym. Lawful access to the content and metadata is minimal, and whilst this varies across popular social messaging applications, Telegram gives authorities the very least in overall comparison[5].

Telegram - the following lawful access limitations exist:
- No message content.
- No contact information is provided for law enforcement to pursue a court order.
- Only “Registration Time Data” is available.
- Telegram may disclose IP address and phone number to relevant authorities for confirmed terrorist investigations.

Over the last few years, across popular instant messaging applications, there has been a replication of cybercriminal content and activity usually found on dark web forums, now appearing on instant messaging applications like Telegram. One reason for this replication is that Telegram is becoming harder for authorities to monitor vs dark web forums. A joint study by the cyber intelligence group

[5] https://uk.pcmag.com/security/137344/fbi-document-shows-how-popular-secure-messaging-apps-stack-up

Cyberint and the Financial Times[6] found that cybercrime trade is now exploding on Telegram, with easily accessible public marketplaces for stolen financial data, personal documents, malware, hacking guides, and online account credentials.

One area of concern is that Telegram allows the creation of public and private broadcast channels where leaked and stolen data is dumped or traded. Users can easily set up an account and promote harmful content using these broadcast channels, acting anonymously, and finding buyers for the information. To locate scam channels, all a user needs to do is search for keywords in the group section of the application. These broadcast channels also act as a gateway to more specific private channels, which are even more challenging to monitor and take down.

Below are some examples of the content found on public scam-related telegram broadcast channels in 2022:

- Full personal and bank login details are offered for purchase through private messages.
- Full technical guides on how to carry out payment reversal fraud across various online retailers.
- Regular posts and dumped lists of complete financial profiles to a channel.
- Posting images of success stories and luxury goods purchased with stolen funds.
- Examples of how to target victims through various social engineering methods.
- Requests for users with active cryptocurrency exchange and TransferWise accounts, with verified ID and deposit history.
- Requests for drop addresses from users.
- UK and Foreign BINs (Bank Information Numbers).

The Telegram broadcast channels also appear to act like organised crime units, where a particular hierarchy exists. The top-level participants remain in control and ultimately remove themselves from the immediate criminal activity. Cybercriminals at the top of the Telegram channel chain act as administrators, recruiting potentially younger users through social media influence to help them launder money, steal crypto assets, or purchase luxury items in return for a percentage fee.

6 Young People and the Excitement of Online Scamming

Increased exposure to social media influence, channels, and cyber scam subculture can further draw young people towards scamming and cybercrime - this is a complex issue:

- We know that there is an acceleration of young people going online and with access to smartphones and the internet.
- It is straightforward to find these channels and learn about scamming techniques, and there is a sense of convenience to making money online and from the home.
- Traditional employment opportunities are constantly changing, and young people may need to look for other income sources, primarily online.
- Boredom and more time spent online can also contribute to individuals investigating new social spaces and communities online.
- Social media influencers and channels can be a gateway for young people, especially those looking to identify themselves online.

[6] https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b

- Using anti-language and slang expressions could contribute to a shared sense of identity within the cyber scam subculture.
- Through studying various Telegram channels, there appears to be evidence of gamification and a collective herd approach occurring through messaging channels.
- Online scamming might also appear acceptable amongst their peer groups the more it appears on social media.
- Online fraud further becomes normalised amongst young people and does not appear as a serious crime, often seen as just something young people do online.
- Online scamming activity, which targets victims in the UK, could quite easily be administered from other foreign geographic locations.

7 What Really Can be Done?

Tech companies and the relevant authorities must work together in a coordinated manner to protect users from accessing harmful content. Unfortunately, this is a complicated cross-border issue that remains difficult to prosecute. Social media and instant messaging companies will always seek out new user growth, which often translates as popularity and market share, and therefore they have removed various registration barriers. Proactive content moderation is seemingly a lower priority, with new fraudulent accounts and replica channels appearing almost immediately after others have disappeared. Through AI-driven fraud detection technology, tech companies may be able to counter account creation misuse and significantly aid content moderation efforts.

There are also challenges with the emerging cyber scam culture and how authorities must continue to modernise and adapt. They may have abundant experience handling traditional crimes but must invest heavily in technical and cultural strategies to combat new online crime patterns and culture, especially among young people. It will also be essential for governments to improve online awareness and continue education campaigns, such as the National Crime Agency (NCA) Cyber Choices programme[7], which aims to help target young people to warn them about the risks of becoming involved with online scams and cybercrime.

The criminal justice system must impose harsher sentences to publicise the damage and harm to victims caused by online fraud and cybercrime. The related authorities will need to carefully inspect fraud survey data to ensure they are not miscalculating official crime figures, which may only show a fraction of actual cases.

Additionally, initiatives such as the DCPCU (Dedicated Card and Payment Crime Unit), a banking industry-funded police unit from UK Finance, will need ongoing, dedicated funding to ensure this unit can significantly aid fraud investigations alongside law enforcement.

In summary:

1. The authorities must invest heavily in technical and cultural strategies to combat online cybercrime culture, especially among young people.

2. Harsher regulatory pressure and controls on tech companies will be needed to prevent social media fraudsters from creating fake accounts and causing harm.

3. To understand the true scale of the problem, we must improve victim protection and crime reporting mechanisms.

Unfortunately, without complete alignment between tech companies and the related authorities, cybercriminals will continue without fear, restriction, or prosecution. Regulatory pressure must be enhanced to force tech companies to remove all scam-related content as soon as it is detected.

[7] https://www.nationalcrimeagency.gov.uk/cyber-choices

Ongoing public education and awareness campaigns will be vital in highlighting the dangers of phishing and online scams, helping protect innocent users from harm, especially those that are more vulnerable.

8 Five Simple Steps to Protect Yourself

1. **Sign up to the Which? Scam Alert Service campaign website**[8]. This online resource provides a regular email newsletter with new trends in online scams and what to look for.

2. **Follow the Take Five campaign's "Stop, Challenge, Protect" guidance**[9]: **Stop**: Pause to think carefully about the current situation. **Challenge**: First, question if this could be a scam. It is ok to reject and ignore a request for information, even if you believe you are talking to an official. **Protect**: Use the number on your bank card to contact your bank directly if you believe you have been involved in an online scam.

3. **Enable Two-Factor Authentication (2FA) for each email account and all of your online website accounts supporting this feature**. Choose a trusted smartphone app, such as Authy[10] or Google Authenticator, instead of SMS text message-based authentication, which is weaker. These mobile authentication applications allow you to generate a thirty-second authentication code for each online website login you use, to guarantee that no unauthorised activity will occur.

4. **Modern smartphones have settings to restrict unknown phone calls** unless a call is from a known number stored in your contact address book. If you receive a suspect email or message, show it to somebody else for a second opinion and try to avoid clicking any links inside the content.

5. **If you receive a phone call, email, or message from someone appearing to be your bank or an organisation you trust, hang up and do not respond to any further communication**. Instead, call your bank directly by finding the official contact number and ask to speak to an advisor. Do not give out authentication or one-time passwords to anyone, as these will never be requested.

Biographies

Sam Ault graduated from Royal Holloway, University of London in 2022 with an MSc in Information Security, where he was awarded a Distinction grade. Sam also holds degrees in Internet Technology from Nottingham Trent University and Anglia Ruskin University, Cambridge. Sam has over a decade of experience in various senior technology roles and is currently consulting as a transformation and leadership coach for a Fortune 500 multinational in the UK, driving transformation strategy across the European e-commerce portfolio. He is passionate about enterprise security awareness and the psychology of human behaviours.

Konstantinos Mersinas, PhD, CISSP, is an Associate Professor at the Information Security Group at Royal Holloway, University of London. Konstantinos has worked in various information security industry roles before moving to academia. A trained mathematician, his research interests lie with behavioural and experimental economics in cybersecurity, decision-making, and cybercrime. His research has been funded by the National Cyber Security Centre in the UK. Konstantinos co-founded the interdisciplinary research group HIVE (the Hub for Interdisciplinary research into Vulnerability to Exploitation) to bridge psychology, law and cybersecurity, and has provided expert feedback for the UK All-Party Parliamentary Group (APPG) on Cybersecurity and for the Fraud Act 2006 and Digital Fraud Committee. He is leading an international project on Digital Trust, across the UK, US and Japan and is a Director at the International Cyber Security Center of Excellence (INCS-CoE.org).

Series editor: Dr Maryam Mehrnezhad, ISG, Royal Holloway

[8] https://www.which.co.uk/consumer-rights/scams

[9] https://www.takefive-stopfraud.org.uk/advice/general-advice/

[10] https://authy.com/