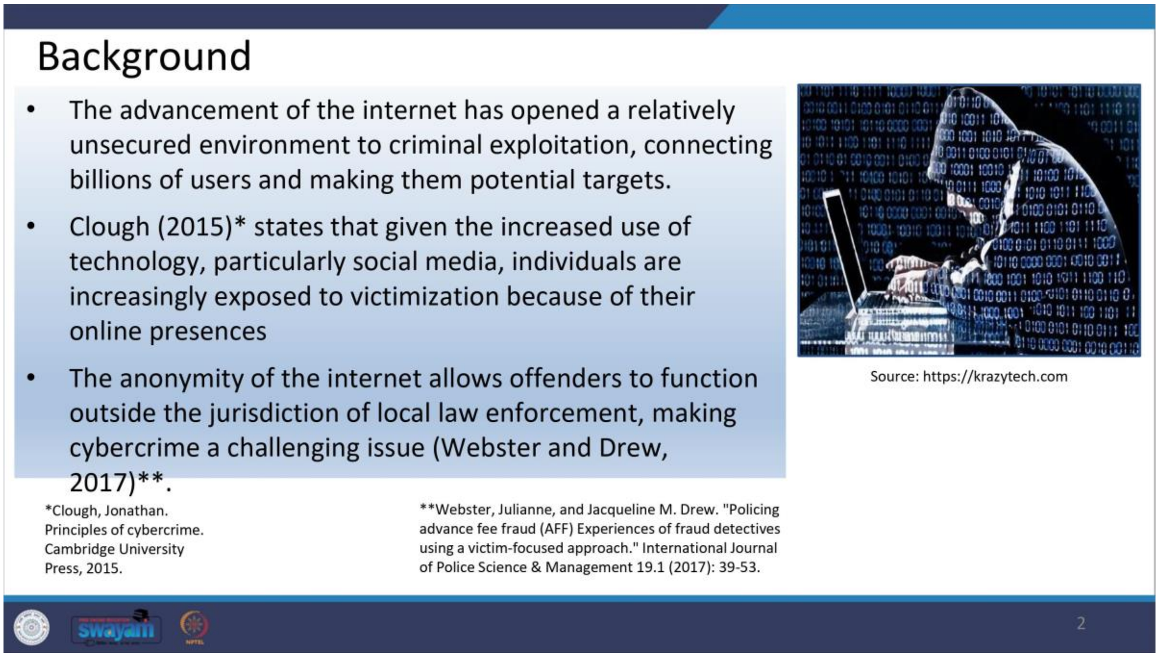
Online Communication in the Digital Age
Prof. Rashmi Gaur
Department of Humanities and Social Sciences
Indian Institute of Technology
Lecture – 46
Scammers and Swindlers in Online Spaces

Good morning and welcome dear friends to our module on Scammers and Scintillas in Online Spaces. Online communication has become an integral part of our lives nowadays and the advancement of the internet has opened a free environment which also connects billions of users simultaneously. However this environment is relatively unsecure and makes the users potential targets to criminal exploitation also. It presents opportunities for scammers and scintillas to exploit unsuspecting individuals.



Background

- The advancement of the internet has opened a relatively unsecured environment to criminal exploitation, connecting billions of users and making them potential targets.
- Clough (2015)* states that given the increased use of technology, particularly social media, individuals are increasingly exposed to victimization because of their online presences
- The anonymity of the internet allows offenders to function outside the jurisdiction of local law enforcement, making cybercrime a challenging issue (Webster and Drew, 2017)**.

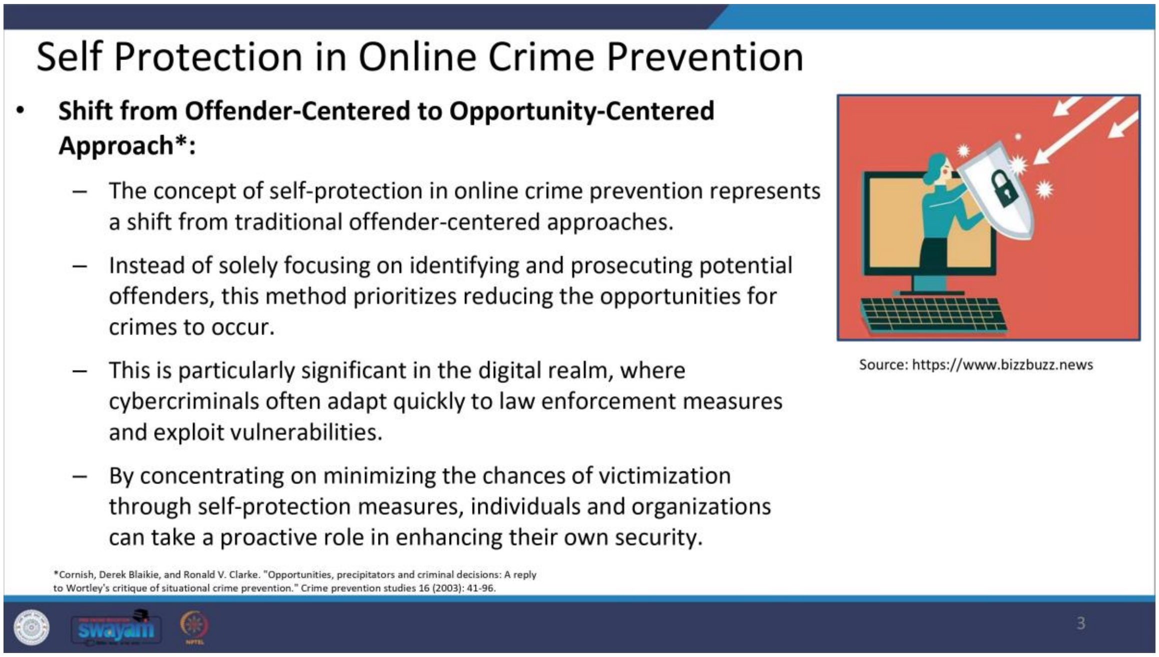
Source: https://krazytech.com

*Clough, Jonathan. Principles of cybercrime. Cambridge University Press, 2015.

**Webster, Julianne, and Jacqueline M. Drew. "Policing advance fee fraud (AFF) Experiences of fraud detectives using a victim-focused approach." International Journal of Police Science & Management 19.1 (2017): 39-53.

Critics like Klaw have suggested that given the increased use of technology, particularly the development in the social media, has exposed the individuals to victimization because of their continuous online footsteps. The anonymity of the internet also allows offenders to function outside the jurisdiction of local law enforcement forces making cybercrime a challenging issue and difficult to solve.

Understanding online scams and scintillas is crucial for protecting ourselves, our finances as well as our personal information. The concept of self-protection in online crime prevention has emerged as a critical paradigm shift in response to the different nature of online crimes.



Self Protection in Online Crime Prevention

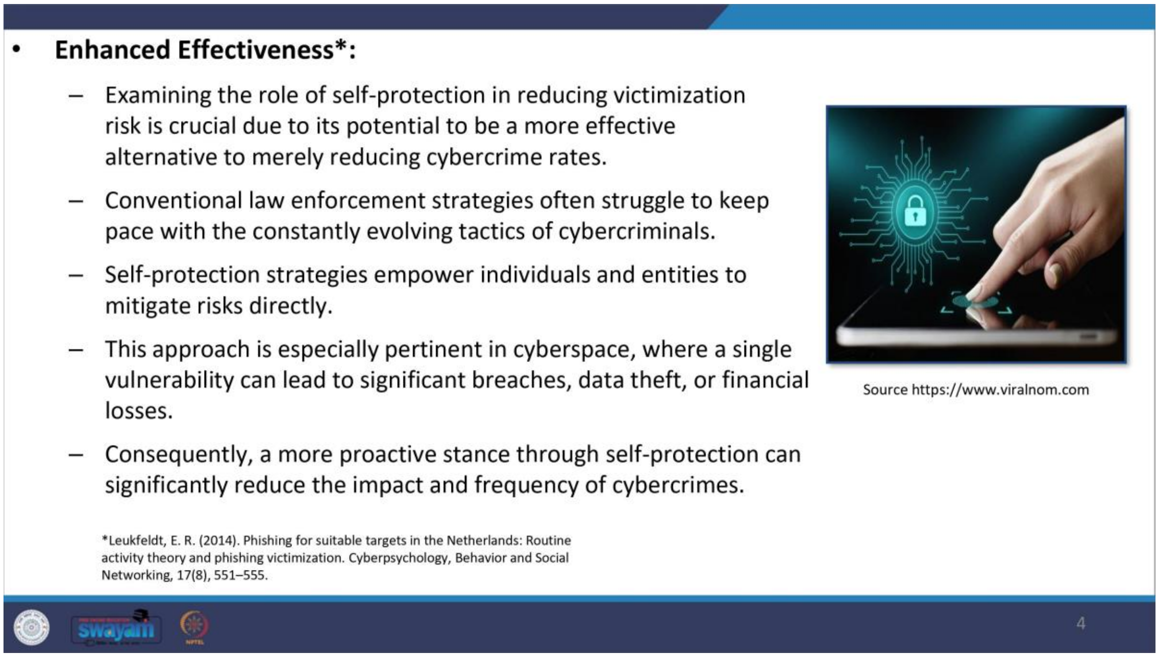
- **Shift from Offender-Centered to Opportunity-Centered Approach*:**
  - The concept of self-protection in online crime prevention represents a shift from traditional offender-centered approaches.
  - Instead of solely focusing on identifying and prosecuting potential offenders, this method prioritizes reducing the opportunities for crimes to occur.
  - This is particularly significant in the digital realm, where cybercriminals often adapt quickly to law enforcement measures and exploit vulnerabilities.
  - By concentrating on minimizing the chances of victimization through self-protection measures, individuals and organizations can take a proactive role in enhancing their own security.

Source: https://www.bizzbuzz.news

*Cornish, Derek Blaikie, and Ronald V. Clarke. "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention." Crime prevention studies 16 (2003): 41-96.

When we talk of self-protection against online crime, then we find that it is drastically different from traditional offender centered approaches. Instead of solely focusing on identifying and prosecuting potential offenders, this method prioritizes reducing the opportunities for crimes to occur by creating an awareness the users. And therefore this is particularly significant in this digital realm where cyber criminals often adapt quickly to law enforcement measures and exploit different kinds of vulnerabilities amongst the people. By concentrating on minimizing the chances of victimization through self-protection measures, individuals and organizations can take a proactive role in enhancing their own security.

Conventional law enforcement agencies often struggle to keep pace with the ever evolving tactics of cyber criminals. Self-protection strategies empower individuals and other entities to mitigate these risks in a direct fashion.



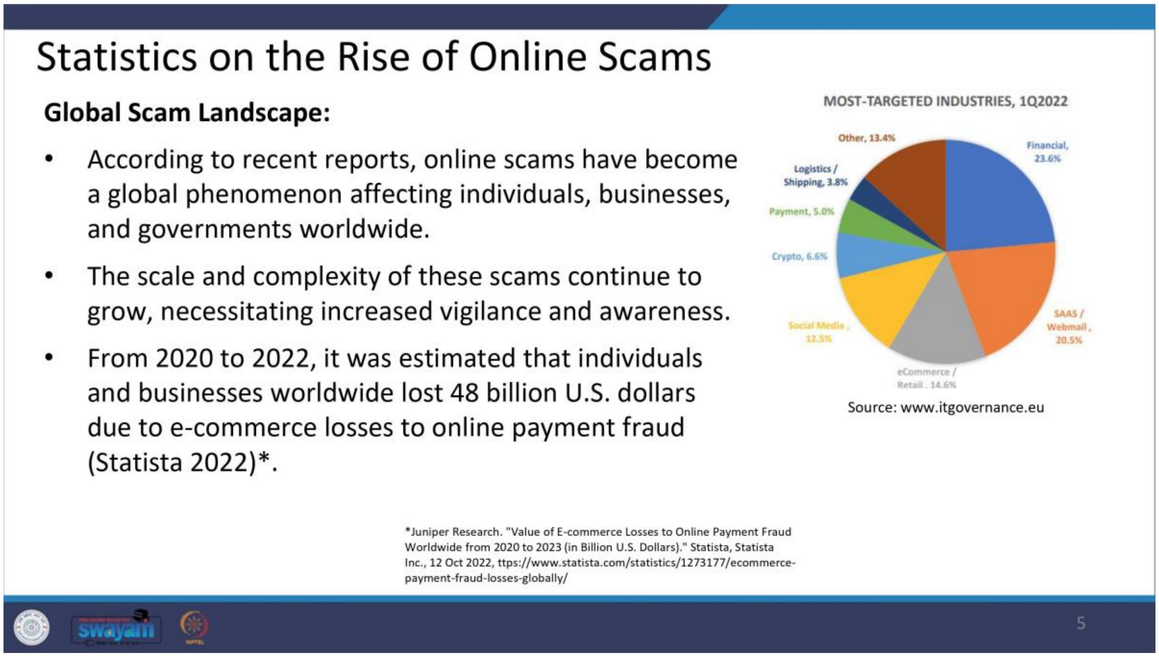
- **Enhanced Effectiveness*:**
  - Examining the role of self-protection in reducing victimization risk is crucial due to its potential to be a more effective alternative to merely reducing cybercrime rates.
  - Conventional law enforcement strategies often struggle to keep pace with the constantly evolving tactics of cybercriminals.
  - Self-protection strategies empower individuals and entities to mitigate risks directly.
  - This approach is especially pertinent in cyberspace, where a single vulnerability can lead to significant breaches, data theft, or financial losses.
  - Consequently, a more proactive stance through self-protection can significantly reduce the impact and frequency of cybercrimes.

Source https://www.viralnom.com

*Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior and Social Networking, 17(8), 551–555.

In the context of online scammers, the law enforcement agencies suggest a more proactive stance through self-protection which would be able to significantly reduce the impact and frequency of cyber crimes. This approach is especially pertinent now where a single weakness of an individual, a single exposed vulnerability can lead to significant breaches, data theft, financial losses and other different types of exploitation.

Online scams have seen a significant increase in recent years causing financial losses and emotional distress for countless individuals. Online scams nowadays have become a global phenomena.



Statistics on the Rise of Online Scams

Global Scam Landscape:

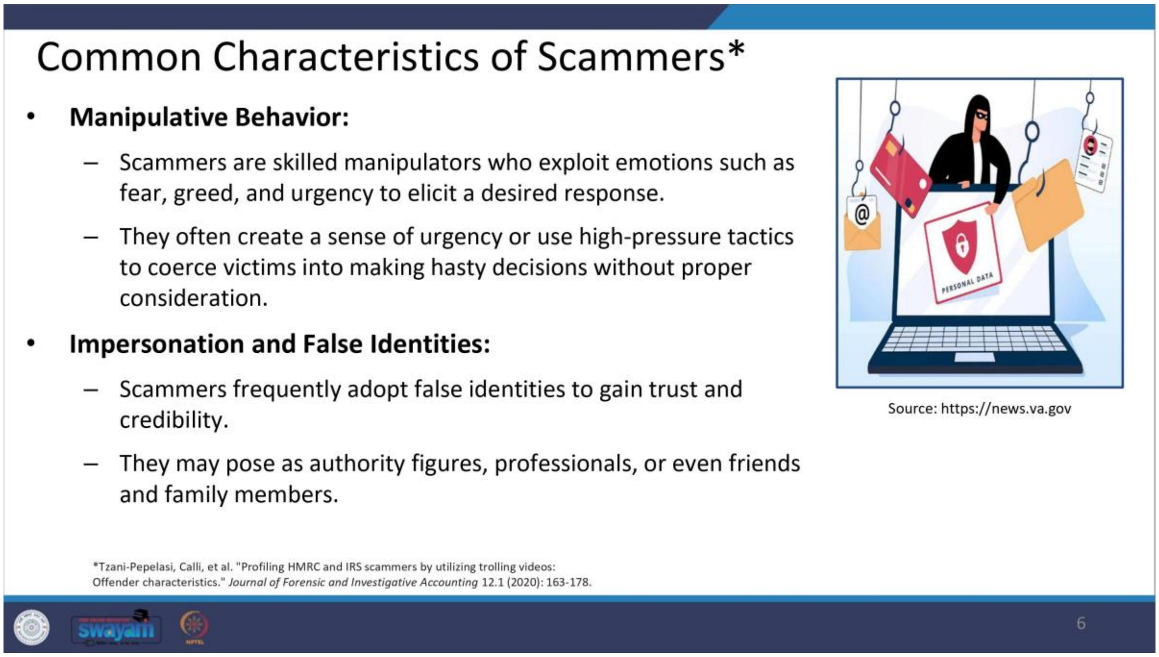
- According to recent reports, online scams have become a global phenomenon affecting individuals, businesses, and governments worldwide.
- The scale and complexity of these scams continue to grow, necessitating increased vigilance and awareness.
- From 2020 to 2022, it was estimated that individuals and businesses worldwide lost 48 billion U.S. dollars due to e-commerce losses to online payment fraud (Statista 2022)*.

Source: www.itgovernance.eu

*Juniper Research. "Value of E-commerce Losses to Online Payment Fraud Worldwide from 2020 to 2023 (in Billion U.S. Dollars)." Statista, Statista Inc., 12 Oct 2022, ttps://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

It affects individuals, businesses and sometimes governments also worldwide. The scale and complexity of these scams continue to grow, necessitating increased vigilance and awareness. In the last two years between 2020 to 2022, it was estimated that individuals and businesses worldwide lost 48 billion US dollars due to losses in e-commerce activities owing to online payment fraud. The figure on the right hand side also illustrates what have been the most targeted industries.

As discussed in earlier modules, scammers often employ specific tactics and exhibit certain common characteristics that can help us in identifying and avoiding falling victim to their schemes.



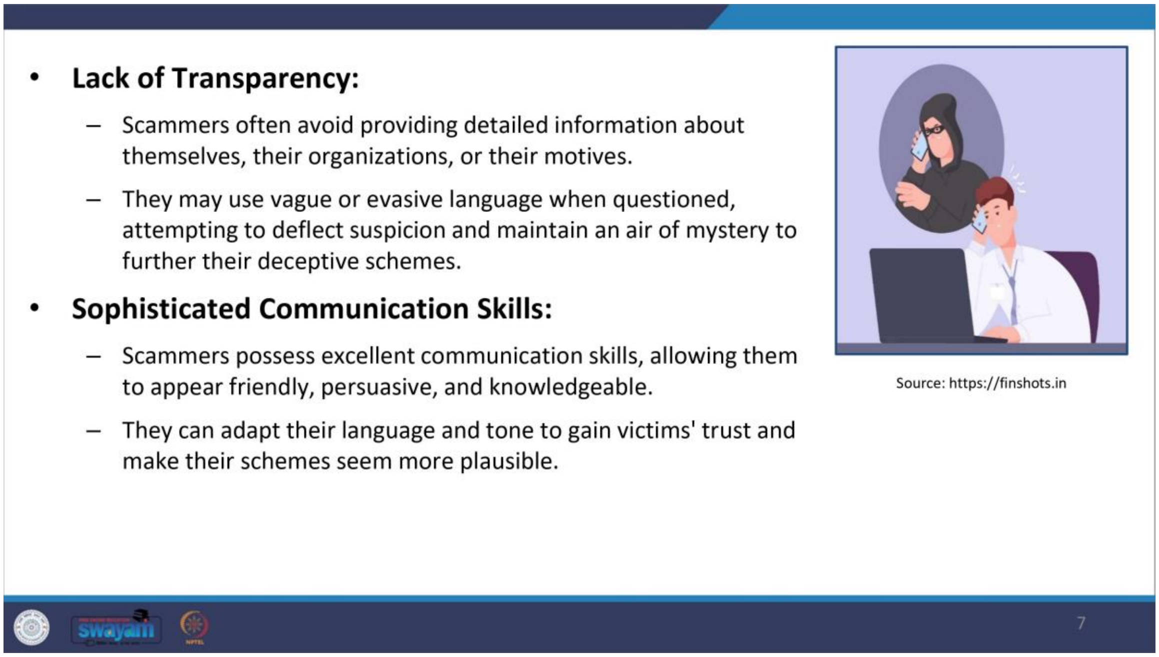
Common Characteristics of Scammers*

- **Manipulative Behavior:**
  - Scammers are skilled manipulators who exploit emotions such as fear, greed, and urgency to elicit a desired response.
  - They often create a sense of urgency or use high-pressure tactics to coerce victims into making hasty decisions without proper consideration.
- **Impersonation and False Identities:**
  - Scammers frequently adopt false identities to gain trust and credibility.
  - They may pose as authority figures, professionals, or even friends and family members.

Source: https://news.va.gov

*Tzani-Pepelasi, Calli, et al. "Profiling HMRC and IRS scammers by utilizing trolling videos: Offender characteristics." *Journal of Forensic and Investigative Accounting* 12.1 (2020): 163-178.

If we try to identify certain common characteristics of scammers, we find that first of all, we have to be aware of their manipulative behavior. Scammers are skilled manipulators who can exploit emotions such as our greed, fear or urgency in order to elicit a desired response. They often also create a sense of urgency or use those tactics which generate a high pressure on individuals so that they are forced to take hasty decisions. They also impersonate and create false identities in order to gain trust and credibility of the people. They often pose as authority figures, professionals or even friends and family members taking advantage of the anonymity afforded by the digital mediums.

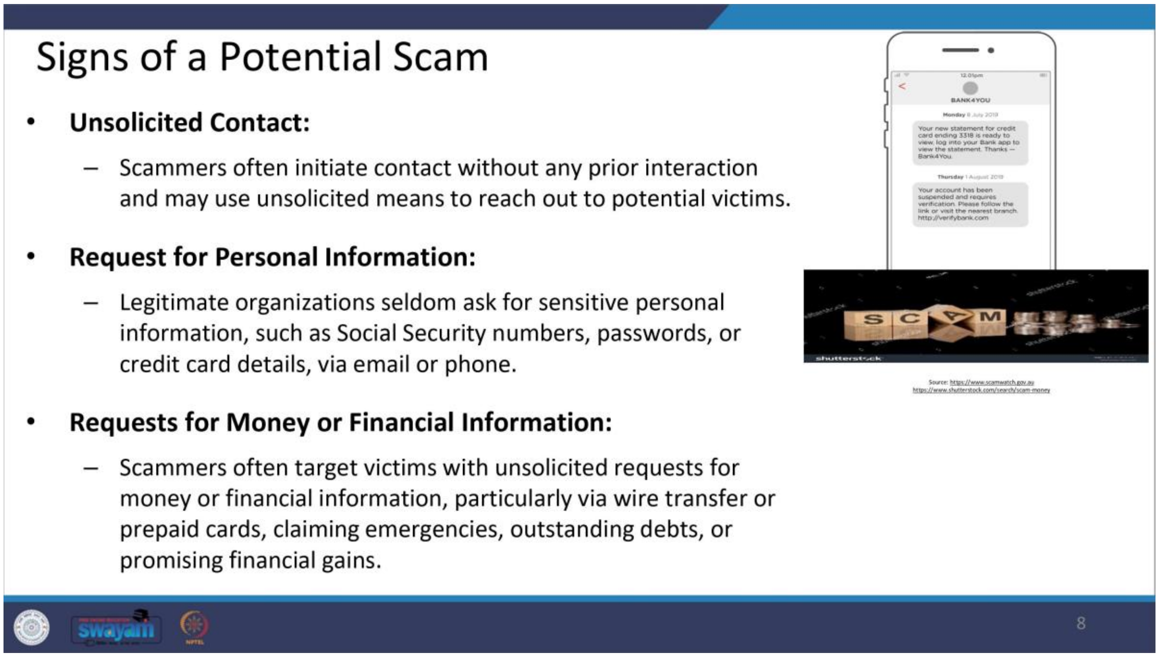


- **Lack of Transparency:**
  - Scammers often avoid providing detailed information about themselves, their organizations, or their motives.
  - They may use vague or evasive language when questioned, attempting to deflect suspicion and maintain an air of mystery to further their deceptive schemes.
- **Sophisticated Communication Skills:**
  - Scammers possess excellent communication skills, allowing them to appear friendly, persuasive, and knowledgeable.
  - They can adapt their language and tone to gain victims' trust and make their schemes seem more plausible.

Source: https://finshots.in

Scammers normally avoid providing a detailed or very precise information about themselves, their organizations or their motives. They use vague and evasive language and when asked a question in a precise manner, they attempt to deflect suspicion and maintain an air of mystery as well as superiority in order to advance their deceptive schemes. They also have highly sophisticated communication skills so that they come across as friendly, persuasive and knowledgeable as well as often as authority figures. They adapt their language and tone to gain the trust of the possible victim and make their scheme seem more plausible.

Understanding these traits is essential for recognizing potential scammers and protecting ourselves from their deceptive practices. Understanding the science of a potential scam is crucial for preventing financial and personal protection.



Signs of a Potential Scam

- **Unsolicited Contact:**
  - Scammers often initiate contact without any prior interaction and may use unsolicited means to reach out to potential victims.
- **Request for Personal Information:**
  - Legitimate organizations seldom ask for sensitive personal information, such as Social Security numbers, passwords, or credit card details, via email or phone.
- **Requests for Money or Financial Information:**
  - Scammers often target victims with unsolicited requests for money or financial information, particularly via wire transfer or prepaid cards, claiming emergencies, outstanding debts, or promising financial gains.

12.01pm

BANK4YOU

Monday 8 July 2019

Your new statement for credit card ending 3318 is ready to view, log into your Bank app to view the statement. Thanks — Bank4You.

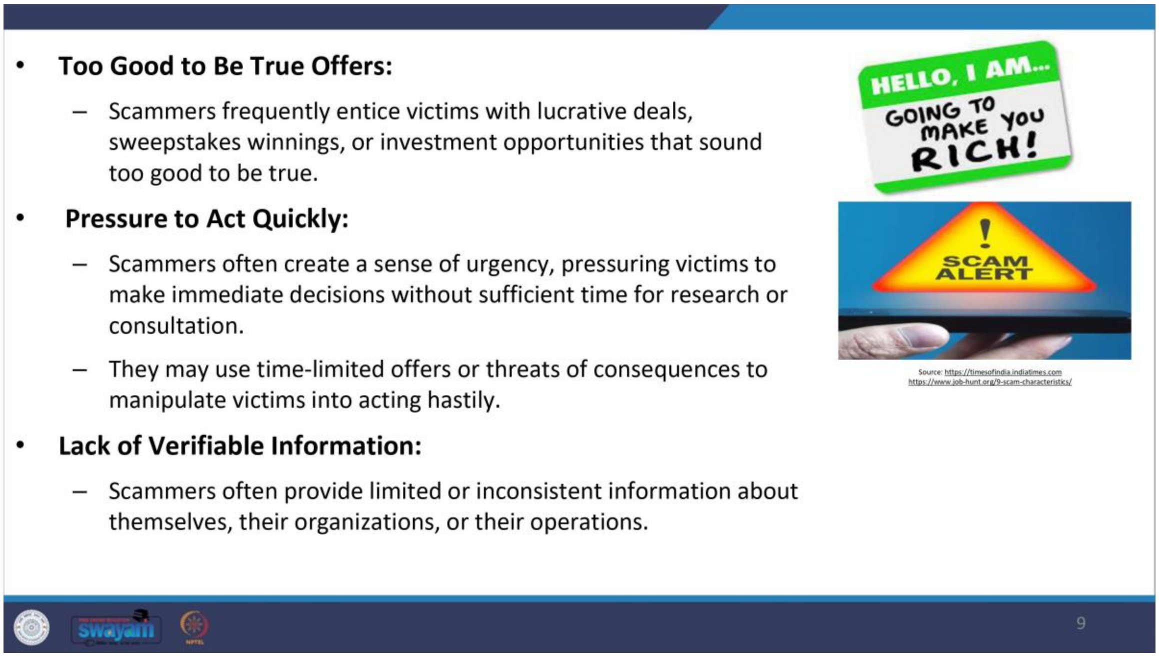
Thursday 1 August 2019

Your account has been suspended and requires verification. Please follow the link or visit the nearest branch. http://verifybank.com

Source: https://www.scamwatch.gov.au
https://www.shutterstock.com/search/scam-money

When we talk about the science of a potential scam, we find that they often begin with an unsolicited contact without any prior interaction.

They normally request for personal information posing on behalf of the legitimate organizations. We find that legitimate organizations seldom ask on phone or social media or internet like emails etc. for sensitive personal information such as social security numbers, passwords or the details of the credit cards. On the other hand, we find that the potential scammers try to find out these details by gaining the trust of the victim. They request for money or financial information.

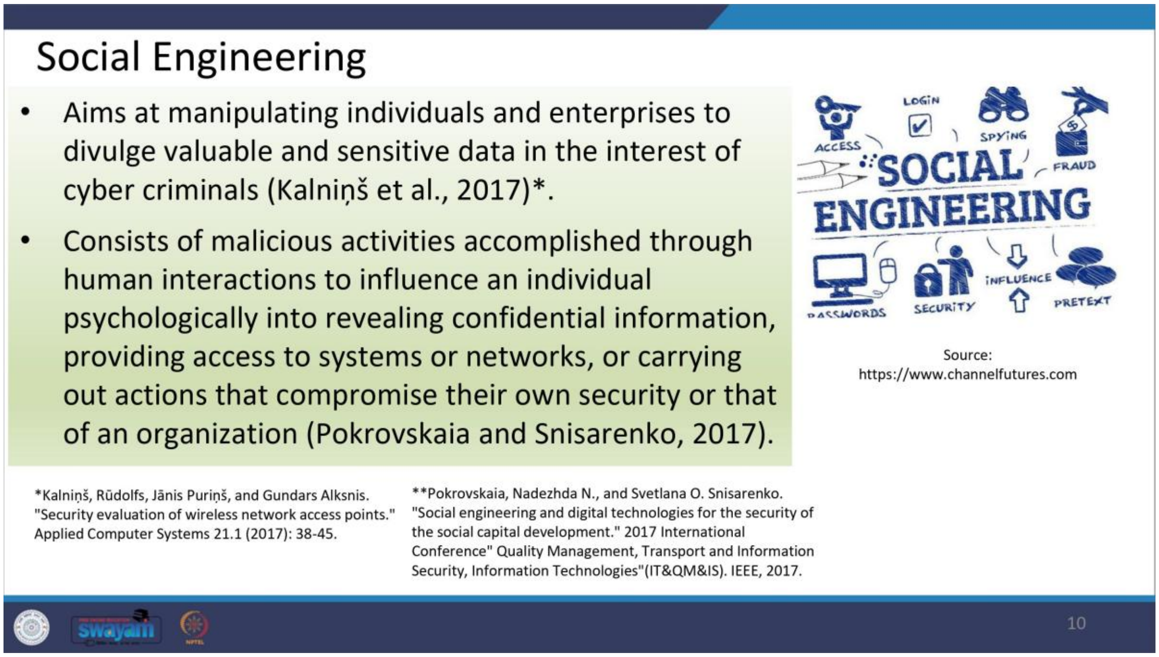

HELLO, I AM...
GOING TO MAKE YOU RICH!
SCAM ALERT

- **Too Good to Be True Offers:**
  - Scammers frequently entice victims with lucrative deals, sweepstakes winnings, or investment opportunities that sound too good to be true.
- **Pressure to Act Quickly:**
  - Scammers often create a sense of urgency, pressuring victims to make immediate decisions without sufficient time for research or consultation.
  - They may use time-limited offers or threats of consequences to manipulate victims into acting hastily.
- **Lack of Verifiable Information:**
  - Scammers often provide limited or inconsistent information about themselves, their organizations, or their operations.

Source: https://timesofindia.indiatimes.com
https://www.job-hunt.org/9-scam-characteristics/

They often request that money should be immediately transferred through wire on prepaid cards claiming emergencies, outstanding debts or promising high financial gains. They often try to entice victims with lucrative deals, sweepstakes winnings or investment opportunities that sound too good to be true. They also try to create a pressure, a sense of emergency on the potential victim in order to act quickly. For this purpose, they also use time limited offers or threats of consequences to manipulate victims into acting hastily without allowing them any time for research or consultation with friends or family. There is also a lack of verifiable information. They often provide either very limited or inconsistent information about themselves, their organizations or their operations. They want to sweet talk the victim or coerce the victim under a sense of false security and the urgency to act immediately.

Scammers often use social engineering which is a form of psychological manipulation. It is a tactic to manipulate individuals into divulging their sensitive information. Through human interaction, they want to psychologically exploit the vulnerabilities of victims, enticing them to share confidential and sensitive information about themselves.



Social Engineering

- Aims at manipulating individuals and enterprises to divulge valuable and sensitive data in the interest of cyber criminals (Kalniņš et al., 2017)*.
- Consists of malicious activities accomplished through human interactions to influence an individual psychologically into revealing confidential information, providing access to systems or networks, or carrying out actions that compromise their own security or that of an organization (Pokrovskaia and Snisarenko, 2017).

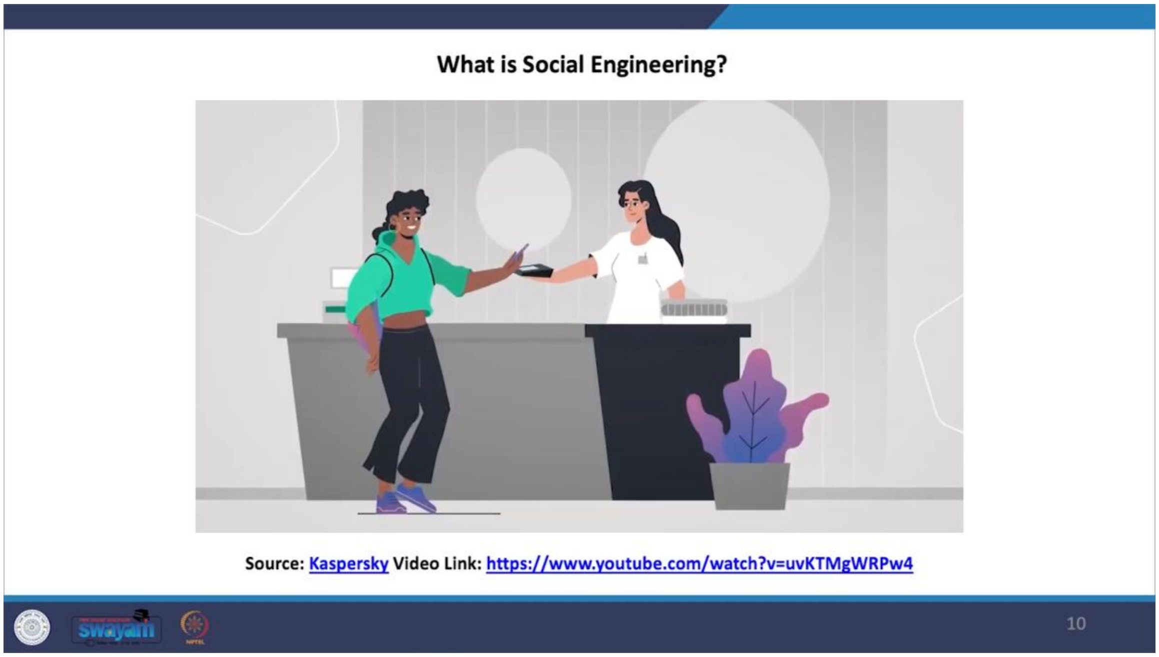
Source: https://www.channelfutures.com

*Kalniņš, Rūdolfs, Jānis Puriņš, and Gundars Alksnis. "Security evaluation of wireless network access points." Applied Computer Systems 21.1 (2017): 38-45.

**Pokrovskaia, Nadezhda N., and Svetlana O. Snisarenko. "Social engineering and digital technologies for the security of the social capital development." 2017 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS). IEEE, 2017.

It consists of malicious activities which are accomplished through human interactions to influence an individual psychologically. And it aims at manipulating individuals and enterprises to share and divulge sensitive data so that the cyber criminal activity can be further perpetuated.

Employment of various social engineering tactics enables these scammers to exploit human susceptibilities of a person's trust and gain illegal access to sensitive details. It also enables a subsequent crime. Let us take a look at a video that explains these tactics briefly.



What is Social Engineering?

Source: Kaspersky Video Link: https://www.youtube.com/watch?v=uvKTMgWRPw4

Has this ever happened to you? You get a text message claiming your debit card may have been used for a fraudulent purchase. The text is urgent and instructs you to text or call a number before more fraudulent charges are posted to your account. You want to stop someone from stealing from you, so it seems like the smart thing to do, right? Wrong. Doing what seems like the right thing in this case is the wrong thing. Why? Because you have been targeted by cyber criminals through social engineering.

Social engineering is a manipulation technique used by cyber criminals. It's where they try to trick you into revealing sensitive information like passwords or credit card data. They may urge you to click on a link or download an attachment or app which will spread malware. They may even try to use you to gain access to restricted systems at your workplace. As with most cyber crime, the purpose of social engineering is to steal information or money from individuals or to sabotage businesses by disrupting or corruption data.

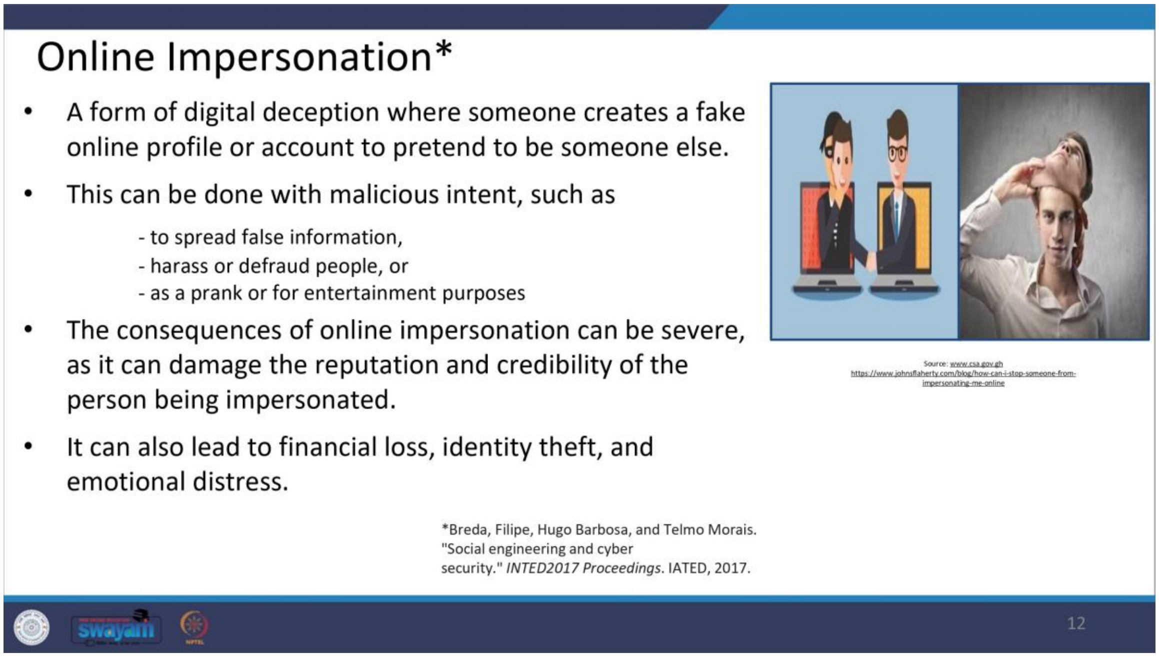
Social engineering is based on human behavior and emotions, how you think and act. Let's look at the three traits of a social engineering attack that play on your emotions. You are more likely to make an irrational or risky choice when you're feeling emotional. For example, you may feel afraid or angry if you get a text claiming someone has used your debit card. You may feel excited or curious if you get an email or a pop-up in your browser claiming you've won something.

Trait number two, urgency. Most fraudulent texts and emails are worded to sound urgent. Your action is required immediately or else you may lose out or something disastrous could happen. Brushing you into a decision overrides your critical thinking ability which can lead to the real disaster. Trait number three, trust.

If an email comes from what seems like a trusted source, double check the URL of the site. Other criminals mimic branded websites and logos but closer inspection usually reveals the website name is slightly different or the images are low resolution. Now that you know the traits of a social engineering attack, you can be on your guard when and where it happens. A social engineering attack can target you through your email, text message or automated voice message. Attacks through websites include DNS spoofing which redirects your browser to malicious websites or scareware.

Scareware uses false warnings that your computer has been infected in order to scare you into purchasing fraudulent cybersecurity software that contains malware. In extreme cases, an attack can be a physical breach of security at a company. Criminals may pose as employees or vendors or may ask you to hold a door open to a restricted area while they carry something in. If you suspect you are being targeted with a social engineering attack, play it cool and take a moment to ask yourself these security questions. Are my emotions heightened? Did this come from a legitimate person or does the email address use characters that mimic others? Would my friend send this? Does the website have an irregular URL, low resolution photos or contain typos? Does the offer sound too good to be true? Does the attachment or link name seem odd or vague? Can this person prove their identity? Be proactive about your privacy and security on your desktop and mobile devices. Playing it cool when you get urgent messages and never sharing your sensitive information is a good place to start. Now that you recognize social engineering, you can avoid it. Protect yourself from social engineering with Kaspersky's products.

Social engineering capitalizes on three key emotional triggers. Beyond emotions, urgency and trust, often mimicking trusted sources. Staying composed, refraining from sharing sensitive data and adopting proactive privacy measures are vital in defending against social engineering. Let us now take a look at the various kinds of online scams that exist. The first type of scam that we will discuss is online impersonations.



Online Impersonation*

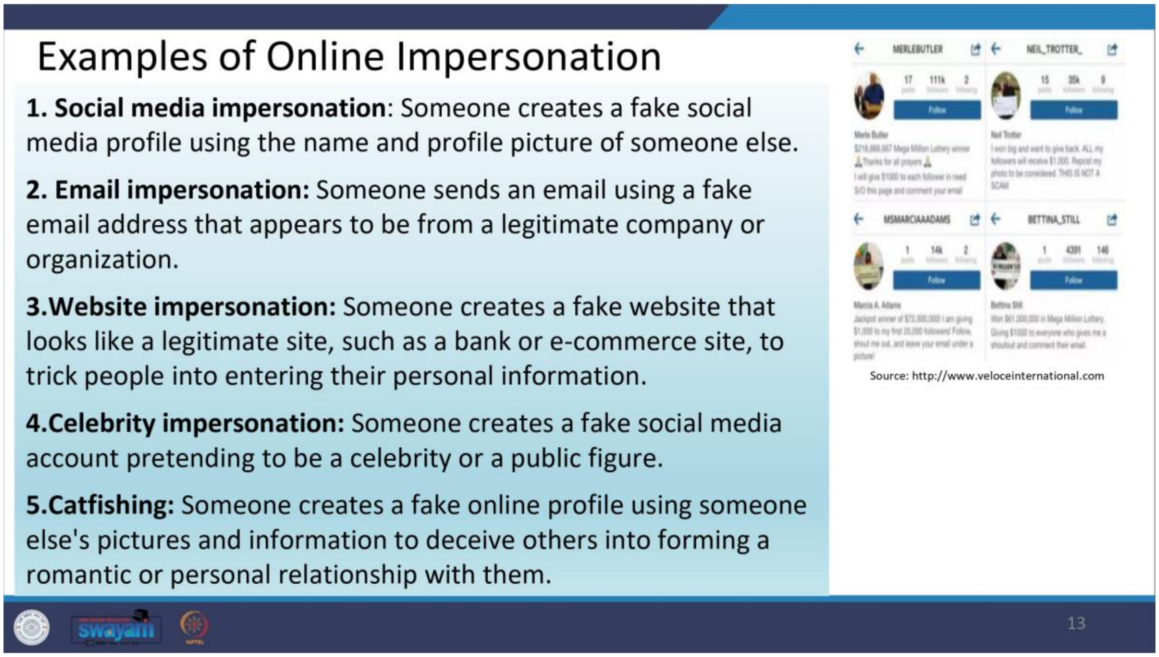
- A form of digital deception where someone creates a fake online profile or account to pretend to be someone else.
- This can be done with malicious intent, such as
  - to spread false information,
  - harass or defraud people, or
  - as a prank or for entertainment purposes
- The consequences of online impersonation can be severe, as it can damage the reputation and credibility of the person being impersonated.
- It can also lead to financial loss, identity theft, and emotional distress.

Source: www.csa.gov.gh
https://www.johnsflaherty.com/blog/how-can-i-stop-someone-from-impersonating-me-online

*Breda, Filipe, Hugo Barbosa, and Telmo Morais. "Social engineering and cyber security." *INTED2017 Proceedings*. IATED, 2017.

Online impersonation is a form of digital deception where someone creates a fake online profile or account to pretend to be somebody else. It can be done with different malicious intentions such as to spread false information to harass or defraud people or as a prank only for entertainment purposes. The consequences of online impersonation can be indeed severe as it can damage the reputation and credibility of the person who is unfortunately being impersonated. It can also lead to financial loss, identity theft and emotional distress as far as the victim is concerned.

Online impersonation can be challenging to detect as the impersonator may often use the same name, profile picture and other personal details as the person they are impersonating. Let us now take a look at some common examples of online impersonation.



Examples of Online Impersonation

1. Social media impersonation: Someone creates a fake social media profile using the name and profile picture of someone else.

2. Email impersonation: Someone sends an email using a fake email address that appears to be from a legitimate company or organization.

3.Website impersonation: Someone creates a fake website that looks like a legitimate site, such as a bank or e-commerce site, to trick people into entering their personal information.

4.Celebrity impersonation: Someone creates a fake social media account pretending to be a celebrity or a public figure.

5.Catfishing: Someone creates a fake online profile using someone else's pictures and information to deceive others into forming a romantic or personal relationship with them.

Merle Butler
$218,666,667 Mega Million Lottery winner
🙏Thanks for all prayers🙏
I will give $1000 to each follower in need
S/O this page and comment your email

Neil Trotter
I won big and want to give back. ALL my followers will receive $1,000. Repost my photo to be considered. THIS IS NOT A SCAM

Marcia A. Adams
Jackpot winner of $72,000,000! I am giving $1,000 to my first 20,000 followers! Follow, shout me out, and leave your email under a picture!

Bettina Still
Won $61,000,000 in Mega Million Lottery. Giving $1000 to everyone who gives me a shoutout and comment their email.

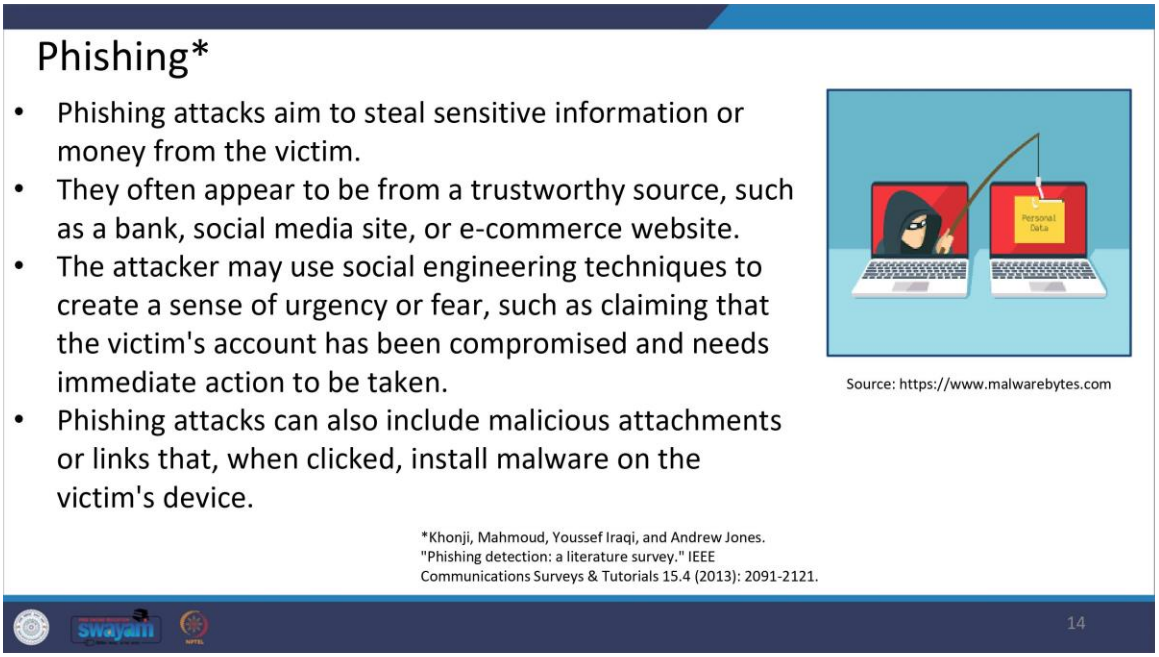
Source: http://www.veloceinternational.com

It can be the form of social media impersonation where someone creates a fake social media profile using the name and profile picture of somebody else.

It can be an email impersonation where somebody sends an email using a fake email address that appears to be from a legitimate company or organization. It can also be in the form of website impersonation where a fake website is created that looks like a legitimate one such as the site of a bank or any e-commerce firm in order to trick people into entering their personal information and fraud them. Celebrity impersonation can also be there where somebody creates a fake social media account pretending to be a celebrity or a public figure. The word catfishing is used when someone creates a fake online profile using someone else's pictures and information to deceive others in forming a romantic or personal relationship with them.

Social media impersonators may use the fake account to harass, to intimidate or to spread false information about the person they are impersonating. Social impersonations may ask for personal information or prompt the recipient to click on a link that installs malware on their device. Malware is a common cyber attack as we know. It is also an umbrella term for various malicious programs which are delivered and installed on end user systems and servers. These attacks are designed and used by cyber criminals to obtain data for financial gain. Malware infects, explores, steals or conducts virtually any behaviour the attacker wants. Website impersonation scams may also use the fake sites to install malware on the device of the victim. Also celebrity impersonators may use fake celebrity accounts to spread false information or scam people out of money by offering fake merchandise or opportunities to meet the celebrity personally. They can be emotionally damaging for the victim when they realise that they have been deceived.

The second type of online scam that we will be discussing is phishing, a form of digital deception where cyber criminals use fraudulent emails, messages or websites to trick individuals into providing personal information such as passwords, credit card information, Aadhaar or PAN number or social security numbers.



Phishing*

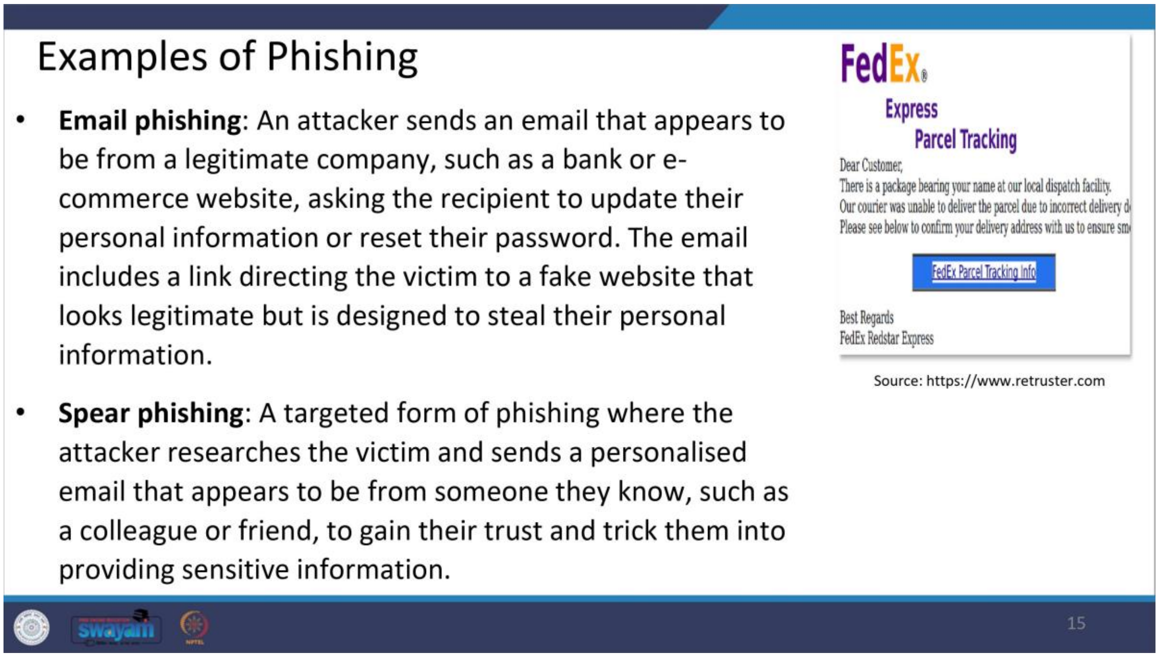
- Phishing attacks aim to steal sensitive information or money from the victim.
- They often appear to be from a trustworthy source, such as a bank, social media site, or e-commerce website.
- The attacker may use social engineering techniques to create a sense of urgency or fear, such as claiming that the victim's account has been compromised and needs immediate action to be taken.
- Phishing attacks can also include malicious attachments or links that, when clicked, install malware on the victim's device.

Source: https://www.malwarebytes.com

*Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing detection: a literature survey." IEEE Communications Surveys & Tutorials 15.4 (2013): 2091-2121.

Phishing attacks often appear to be from a trustworthy source such as a bank or a known social media site or a famous e-commerce website. The attacker may use social engineering techniques to create a sense of urgency or fear or a lucrative offer such as claiming that the victim's account has been compromised and needs immediate action to be taken. Phishing attacks can also include malicious attachments or links that when clicked install malware on the victim's device.

Let us look at some examples that explains the various kinds of phishing techniques.



Examples of Phishing

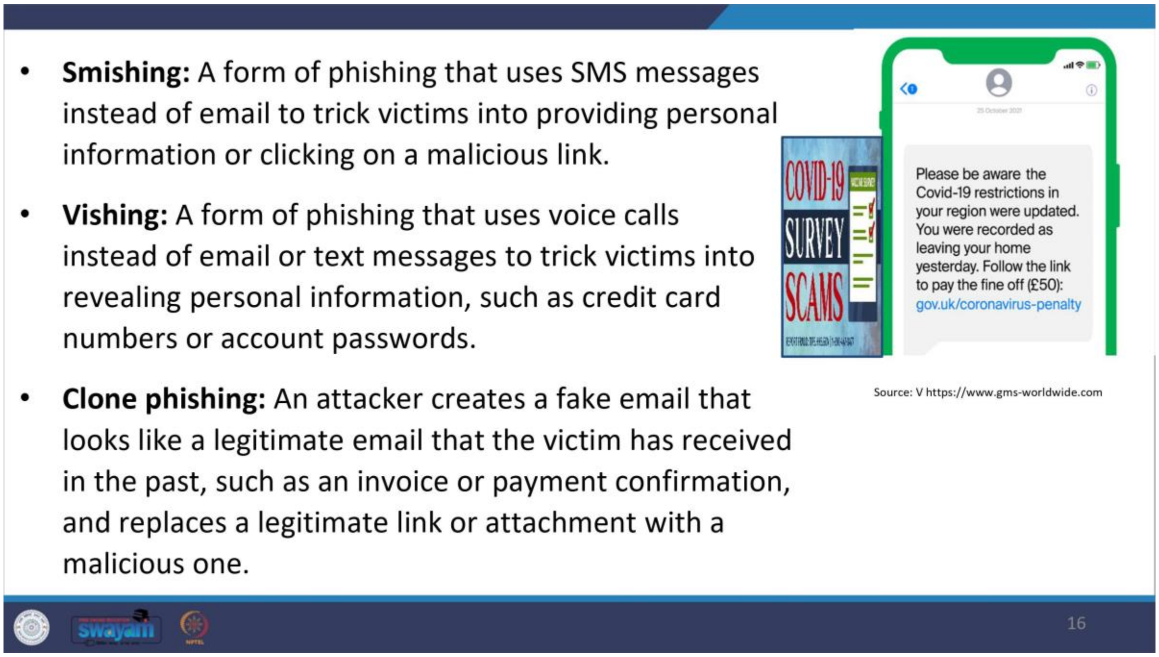
- **Email phishing**: An attacker sends an email that appears to be from a legitimate company, such as a bank or e-commerce website, asking the recipient to update their personal information or reset their password. The email includes a link directing the victim to a fake website that looks legitimate but is designed to steal their personal information.
- **Spear phishing**: A targeted form of phishing where the attacker researches the victim and sends a personalised email that appears to be from someone they know, such as a colleague or friend, to gain their trust and trick them into providing sensitive information.

Dear Customer,
There is a package bearing your name at our local dispatch facility.
Our courier was unable to deliver the parcel due to incorrect delivery d
Please see below to confirm your delivery address with us to ensure sm

Best Regards
FedEx Redstar Express

Source: https://www.retruster.com

Email phishing is very common. An attacker sends an email that appears to be from a legitimate source asking the recipient to update their personal information or to reset their passwords. This also often includes a link directing the victim to a fake website that looks legitimate but is designed to steal their personal information and initiate financial frauds. Spear phishing is known as a targeted form of phishing where the attacker searches the victim and sends a personalized email that appears to be from someone they know such as a colleague or a friend or a family member to gain their trust and trick them into providing sensitive information.



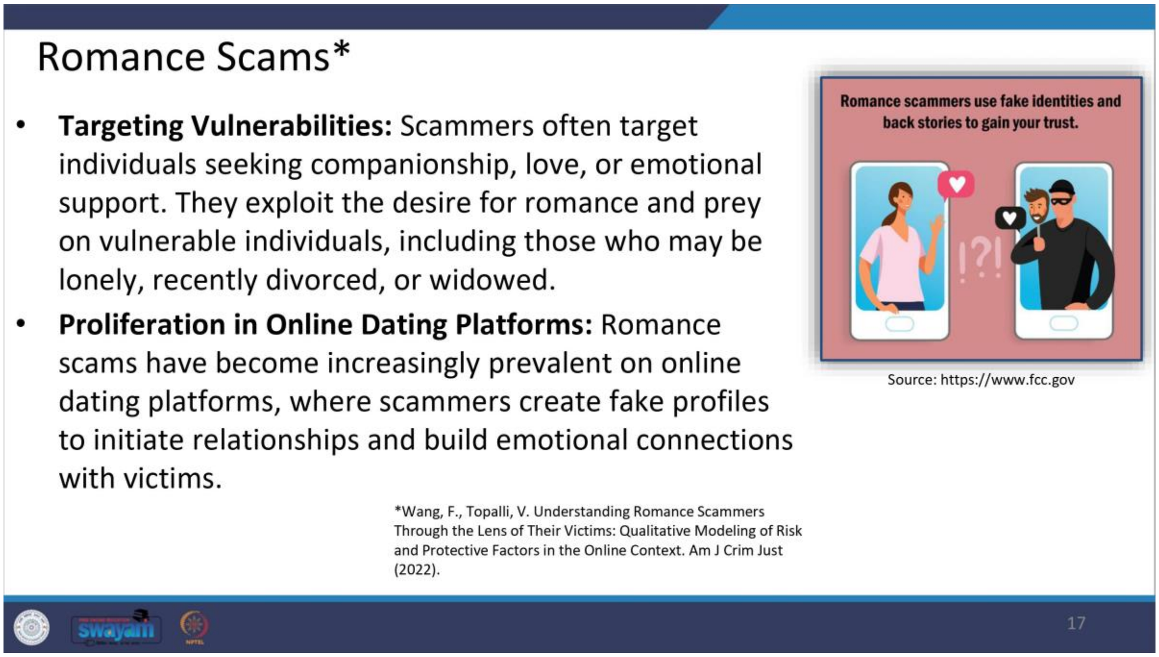
- **Smishing:** A form of phishing that uses SMS messages instead of email to trick victims into providing personal information or clicking on a malicious link.
- **Vishing:** A form of phishing that uses voice calls instead of email or text messages to trick victims into revealing personal information, such as credit card numbers or account passwords.
- **Clone phishing:** An attacker creates a fake email that looks like a legitimate email that the victim has received in the past, such as an invoice or payment confirmation, and replaces a legitimate link or attachment with a malicious one.

Please be aware the Covid-19 restrictions in your region were updated. You were recorded as leaving your home yesterday. Follow the link to pay the fine off (£50): gov.uk/coronavirus-penalty

Source: V https://www.gms-worldwide.com

Smishing is a form of phishing that uses SMS messages instead of email to trick victims into providing personal information or clicking on a malicious link. Vishing uses voice calls instead of email or text messages to trick victims. Clone phishing occurs when an attacker creates a fake email that looks like a legitimate email that the victim has already received in the past such as an invoice or payment confirmation and replaces a legitimate link or attachment with a malicious one.

The third type of online scams we will be discussing are the popular romance scams. Romance scams involve fraudsters creating fake online profiles and engaging in emotional manipulation to exploit victims' trust and affection for financial gain or also for any other type of physical or emotional exploitation.



Romance Scams*

- **Targeting Vulnerabilities:** Scammers often target individuals seeking companionship, love, or emotional support. They exploit the desire for romance and prey on vulnerable individuals, including those who may be lonely, recently divorced, or widowed.
- **Proliferation in Online Dating Platforms:** Romance scams have become increasingly prevalent on online dating platforms, where scammers create fake profiles to initiate relationships and build emotional connections with victims.

Romance scammers use fake identities and back stories to gain your trust.

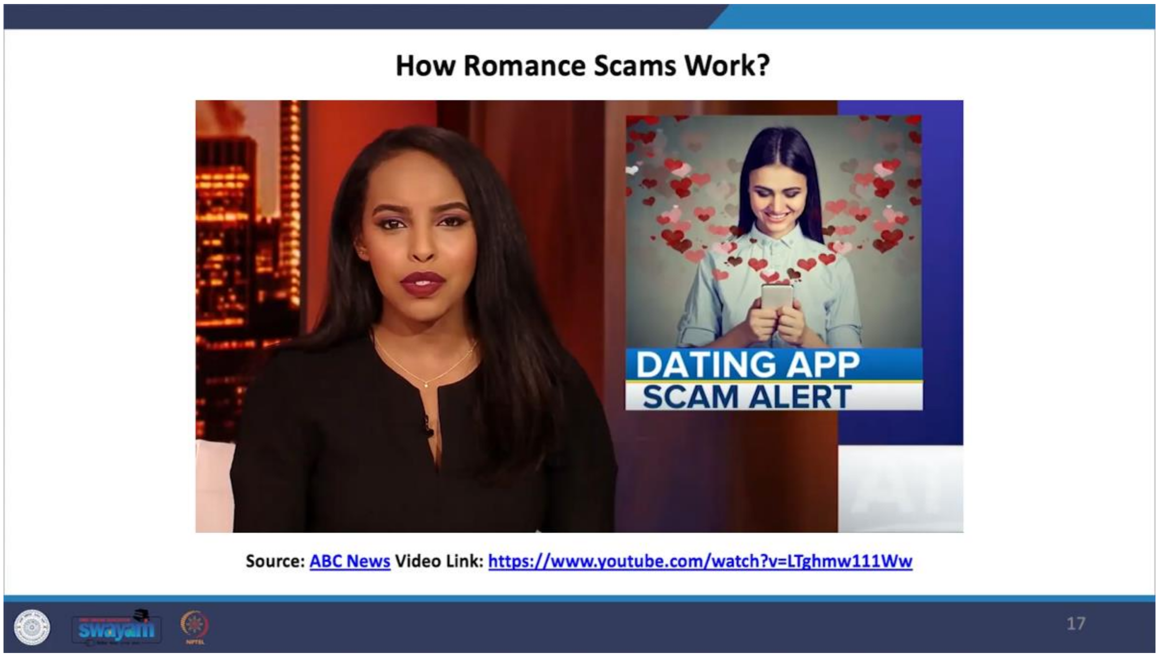
Source: https://www.fcc.gov

*Wang, F., Topalli, V. Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context. Am J Crim Just (2022).

17

In the first method, we find that scammers often target individuals seeking companionship, love or emotional support, etc. They exploit an individual's desire for romance and prey on vulnerable individuals including those who may be lonely, recently divorced or widowed, etc. The proliferation in online dating platforms has also encouraged these scammers and romance scams have become increasingly prevalent on these platforms. The scammers often create fake profiles to initiate relationships and build emotional connections with victims.

Let us take a look at a short video that further explains the concept.



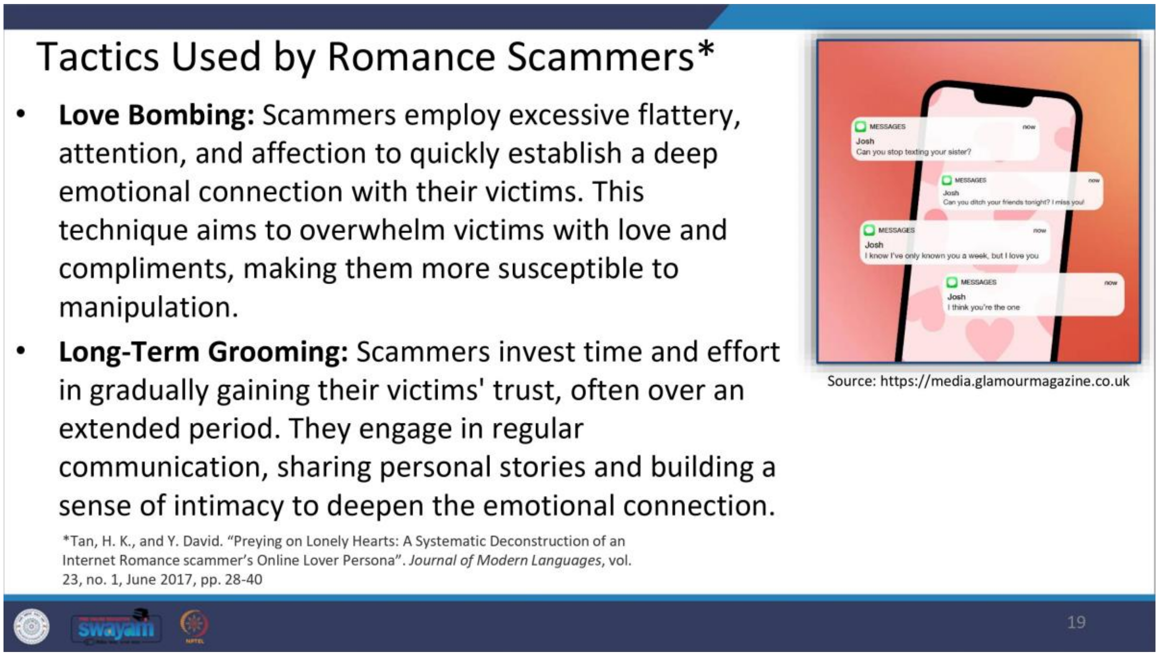
How Romance Scams Work?

Source: ABC News Video Link: https://www.youtube.com/watch?v=LTghmw111Ww

Scammers tries to lure you to a texting app like WhatsApp. That's when they bring up cryptocurrency, convincing victims they've got the inside track on how to make big bucks.

All you need to do is invest. Once you make a deposit, your money is gone. As the popularity of cryptocurrency soars, so do reports of scammers stealing money. The FTC is reporting just last year, losses totaled a staggering $139 million, with victims on average losing nearly $10,000. The big rage when I was a kid was the Nigerian Prince scam. You know, somebody would spend $10,000 to depose the King of Nigeria.

It's that same line of scam. A search of the BBB's scam tracker shows one victim lost $270,000. After a scammer they met on a dating app told them to invest in crypto. So what can you do to prevent being ripped off? Never send money to someone you haven't met in person, even if your heart says yes. Consult a financial advisor, consult family members, you should talk to people before engaging in these types of actions. If someone's asking you for digital currency or crypto and you've never met them in person or known them only a short time, this is a huge red flag and you should walk away.



Tactics Used by Romance Scammers*

- **Love Bombing:** Scammers employ excessive flattery, attention, and affection to quickly establish a deep emotional connection with their victims. This technique aims to overwhelm victims with love and compliments, making them more susceptible to manipulation.
- **Long-Term Grooming:** Scammers invest time and effort in gradually gaining their victims' trust, often over an extended period. They engage in regular communication, sharing personal stories and building a sense of intimacy to deepen the emotional connection.

MESSAGES now
Josh
Can you stop texting your sister?

MESSAGES now
Josh
Can you ditch your friends tonight? I miss you!

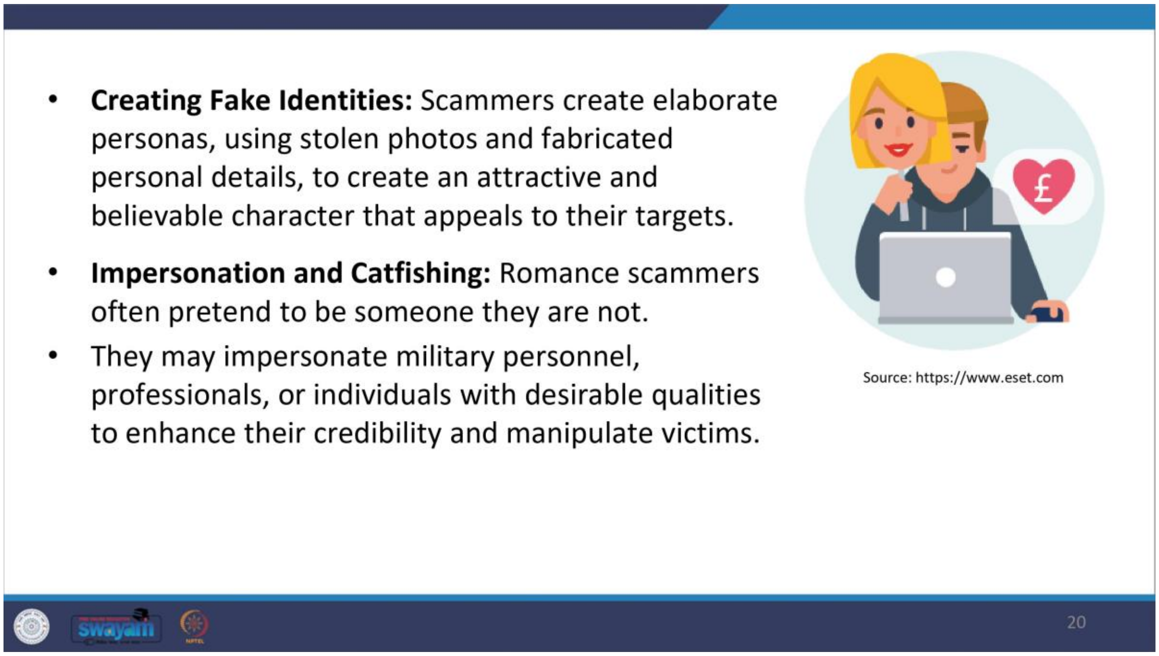
MESSAGES now
Josh
I know I've only known you a week, but I love you

MESSAGES now
Josh
I think you're the one

Source: https://media.glamourmagazine.co.uk

*Tan, H. K., and Y. David. "Preying on Lonely Hearts: A Systematic Deconstruction of an Internet Romance scammer's Online Lover Persona". *Journal of Modern Languages*, vol. 23, no. 1, June 2017, pp. 28-40

Romance scammers employ specific tactics to manipulate victims and gain their trust. They may use excessive flattery, attention and affection to quickly establish a deep emotional connection with their victims. Or on the other hand, they can invest time and effort in gradually gaining the trust of the victim and isolate these potential victims from their friend and family over an extended period of time. They engage in regular communication, sharing personal stories and building a sense of intimacy. The first type of scam is known as love bombing, whereas the second style is known as long term grooming.

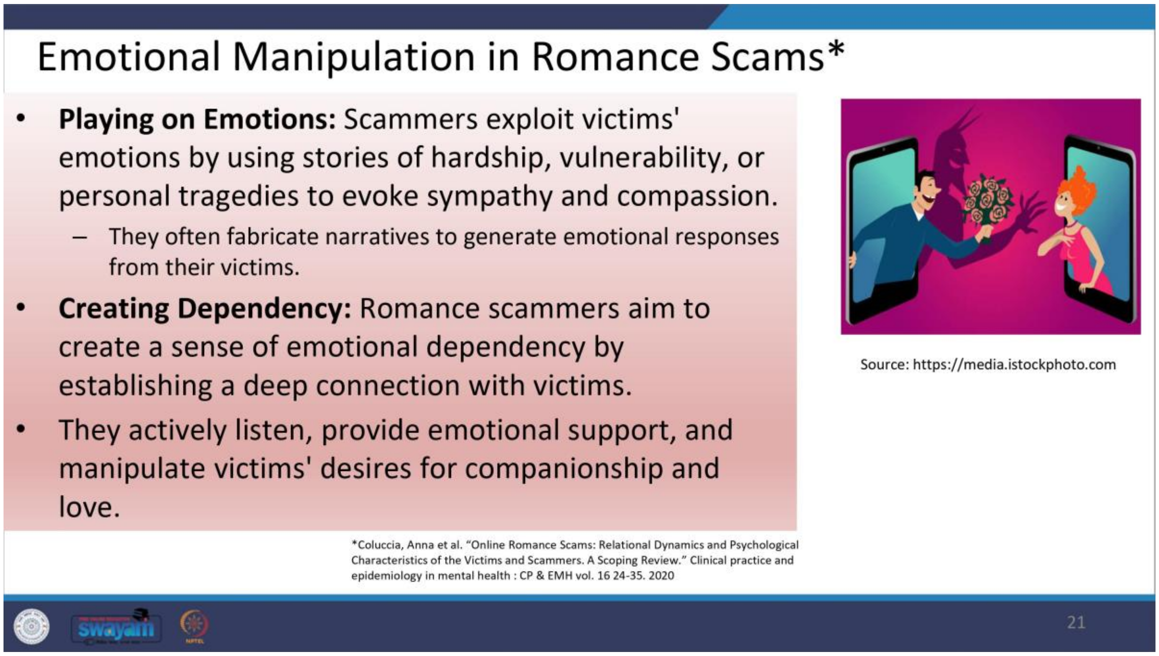


- **Creating Fake Identities:** Scammers create elaborate personas, using stolen photos and fabricated personal details, to create an attractive and believable character that appeals to their targets.
- **Impersonation and Catfishing:** Romance scammers often pretend to be someone they are not.
- They may impersonate military personnel, professionals, or individuals with desirable qualities to enhance their credibility and manipulate victims.

Source: https://www.eset.com

Using different and detailed techniques, scammers create elaborate personas using stolen photographs and fabricated personal details to create an attractive and believable character that appeals to their targets. Romance scammers often pretend to be someone they are not. They may impersonate those professions which are highly respected in the society. For example, military personnel, professionals or individuals with desirable qualities to enhance their credibility and to manipulate victims.

Being aware of these tactics can help us in recognizing and avoiding such scams. Emotional manipulation is a key element of all types of romance scams. As scammers exploit the emotions of the victims to control their actions for their exploitation.



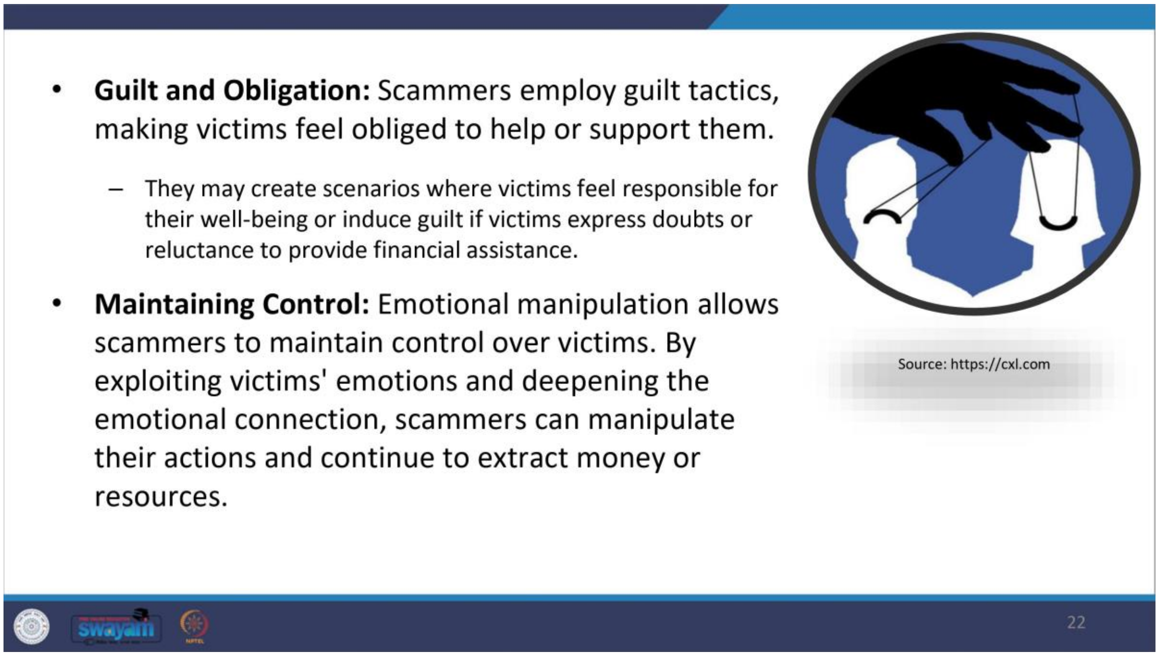
Emotional Manipulation in Romance Scams*

- **Playing on Emotions:** Scammers exploit victims' emotions by using stories of hardship, vulnerability, or personal tragedies to evoke sympathy and compassion.
  – They often fabricate narratives to generate emotional responses from their victims.
- **Creating Dependency:** Romance scammers aim to create a sense of emotional dependency by establishing a deep connection with victims.
- They actively listen, provide emotional support, and manipulate victims' desires for companionship and love.

Source: https://media.istockphoto.com

*Coluccia, Anna et al. "Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review." Clinical practice and epidemiology in mental health : CP & EMH vol. 16 24-35. 2020

By using stories of hardship, difficulties and personal tragedies, these scammers often want to exploit the emotions of the targeted victims in order to evoke sympathy and compassion. They also create a sense of emotional dependency by establishing a deep connection over a passage of time with victims. They actively listen, provide emotional support, provide a shoulder to cry on and thus manipulate the desires of the victims for companionship, love and romance. Scammers also often use guilt tactics making victims feel obliged to help or support them. They create scenarios where victims feel responsible for the well-being of the scammers or induce guilt if victims express doubts or certain reluctance to provide financial assistance. Such techniques of emotional manipulation allow scammers to maintain control over victims. By exploiting their emotions and deepening the emotional connection, scammers can manipulate their actions and continue to extract money or other types of resources.

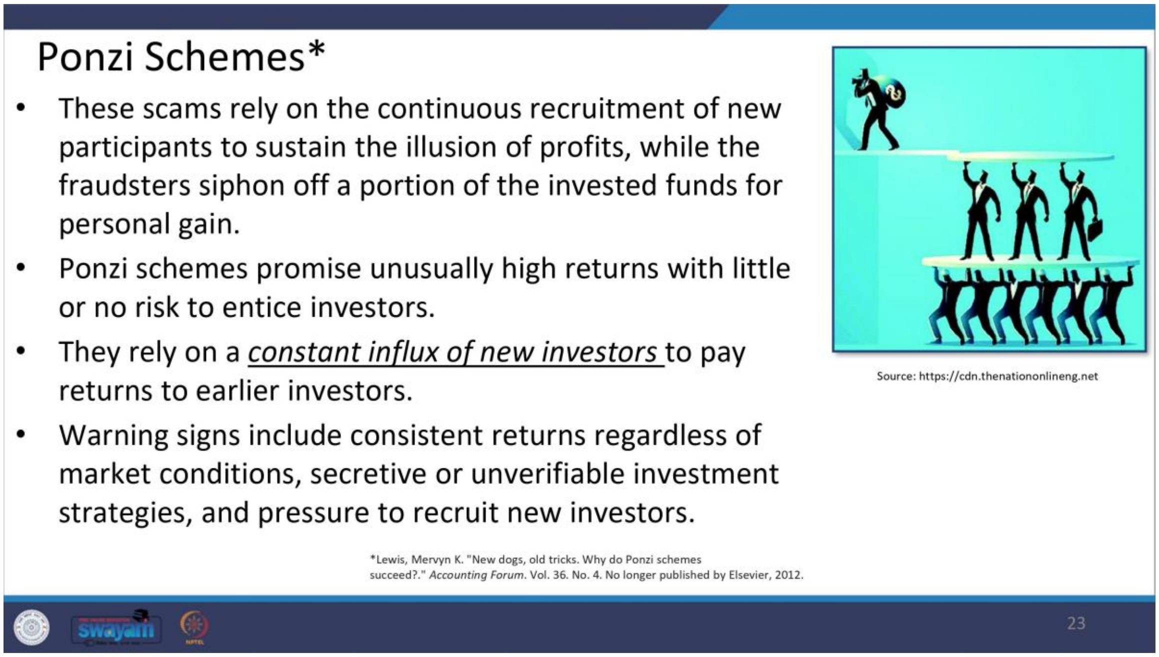


- **Guilt and Obligation:** Scammers employ guilt tactics, making victims feel obliged to help or support them.
  - They may create scenarios where victims feel responsible for their well-being or induce guilt if victims express doubts or reluctance to provide financial assistance.
- **Maintaining Control:** Emotional manipulation allows scammers to maintain control over victims. By exploiting victims' emotions and deepening the emotional connection, scammers can manipulate their actions and continue to extract money or resources.

Source: https://cxl.com

Romance scams can have devastating financial and emotional consequences for victims. It is crucial to be cautious when developing relationships online, verify the authenticity of individuals and refrain from sending money or sharing personal information or personal photographs with individuals you have not actually met in person.

Finally, investment scams lure individuals with promises of high returns and low risks. But in reality, they are schemes designed to defraud unsuspecting victims.



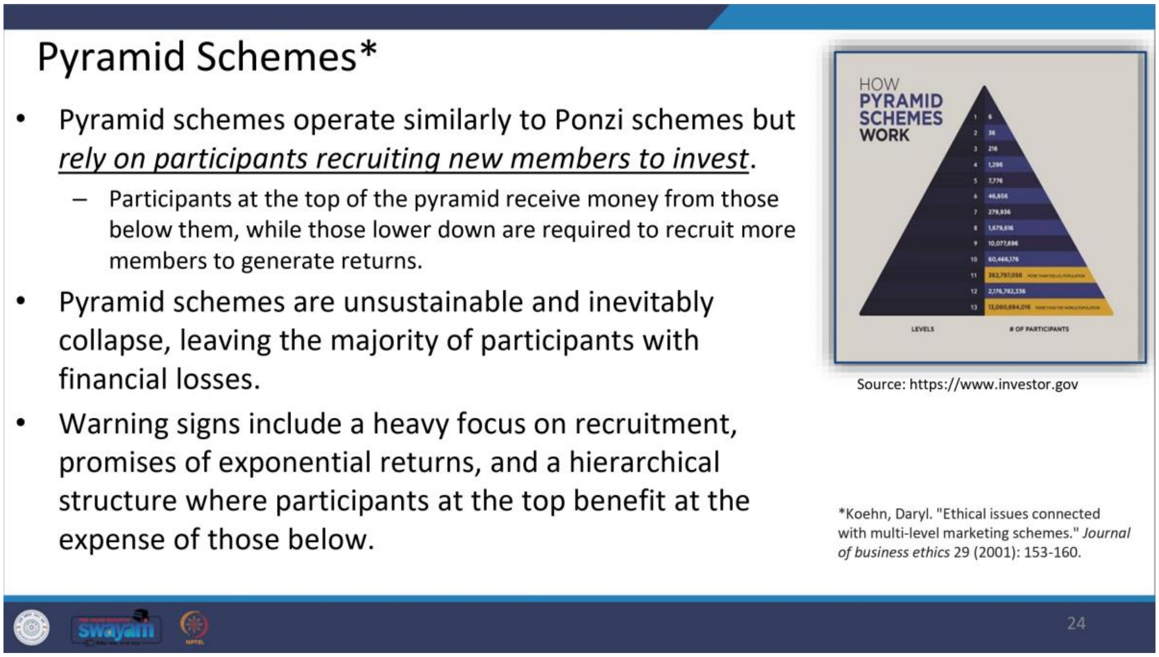
Ponzi Schemes*

- These scams rely on the continuous recruitment of new participants to sustain the illusion of profits, while the fraudsters siphon off a portion of the invested funds for personal gain.
- Ponzi schemes promise unusually high returns with little or no risk to entice investors.
- They rely on a *constant influx of new investors* to pay returns to earlier investors.
- Warning signs include consistent returns regardless of market conditions, secretive or unverifiable investment strategies, and pressure to recruit new investors.

Source: https://cdn.thenationonlineng.net

*Lewis, Mervyn K. "New dogs, old tricks. Why do Ponzi schemes succeed?." *Accounting Forum*. Vol. 36. No. 4. No longer published by Elsevier, 2012.

All of us are familiar with Ponzi schemes. Ponzi schemes promise unusually high returns with little or no risk to entice investors. They rely on a constant flux of new investors to pay returns to earlier investors and also they keep on continually recruiting new participants to sustain the illusion of profits while the fraudsters siphon off a portion of the invested funds for personal gain. The warning signs in these Ponzi schemes include consistent returns regardless of market conditions, secretive or unverifiable investment strategies and a continuous pressure to recruit new investors.



Pyramid Schemes*

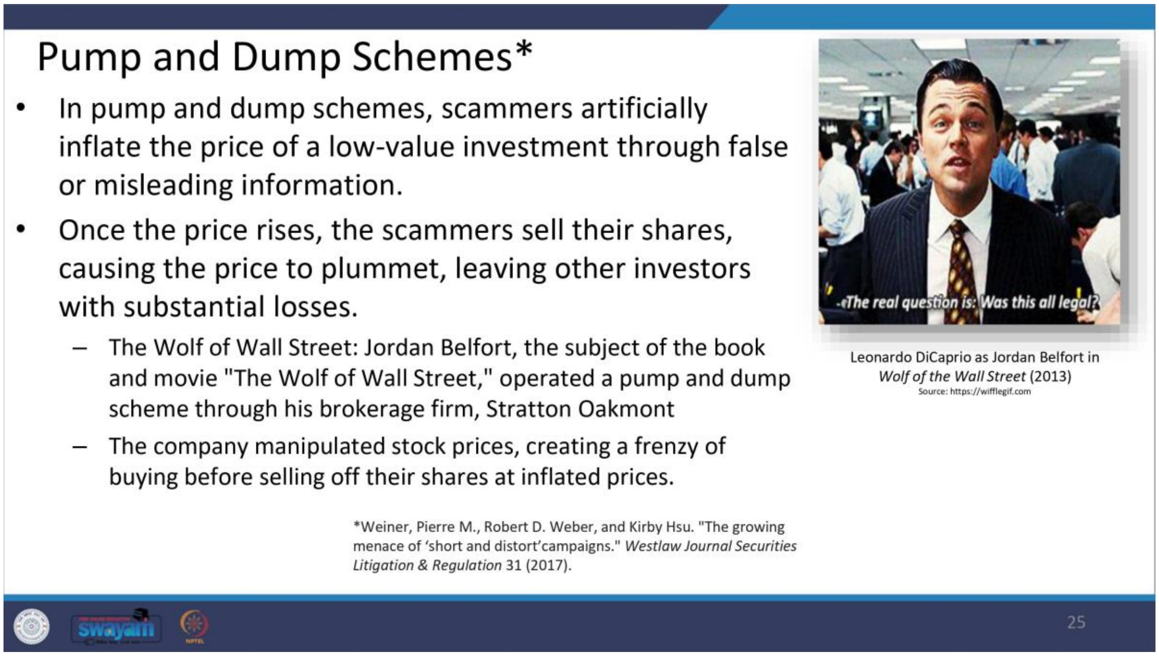
- Pyramid schemes operate similarly to Ponzi schemes but *rely on participants recruiting new members to invest*.
  - Participants at the top of the pyramid receive money from those below them, while those lower down are required to recruit more members to generate returns.
- Pyramid schemes are unsustainable and inevitably collapse, leaving the majority of participants with financial losses.
- Warning signs include a heavy focus on recruitment, promises of exponential returns, and a hierarchical structure where participants at the top benefit at the expense of those below.

Source: https://www.investor.gov

*Koehn, Daryl. "Ethical issues connected with multi-level marketing schemes." *Journal of business ethics* 29 (2001): 153-160.

Similarly, pyramid schemes are also used. They operate similarly to Ponzi schemes but unlike them, rely on participants recruiting new members to invest. Participants at the top of the pyramid receive money from those below them while those lower down are required to recruit more members to continually generate returns. These schemes are unsustainable and inevitably collapse leaving the majority of participants with financial losses. Warning signs about pyramid schemes include a heavy focus on recruitment, promises of exceptional returns and a hierarchical structure where participants at the top benefit at the expense of those below.

Both Ponzi and pyramid schemes are illegal and unsustainable. As new investors dry up, the schemes collapse leaving the majority of participants with significant financial losses. Victims often face difficulties in recovering their investments as the fraudsters typically dissipate funds or hide their assets.



Pump and Dump Schemes*

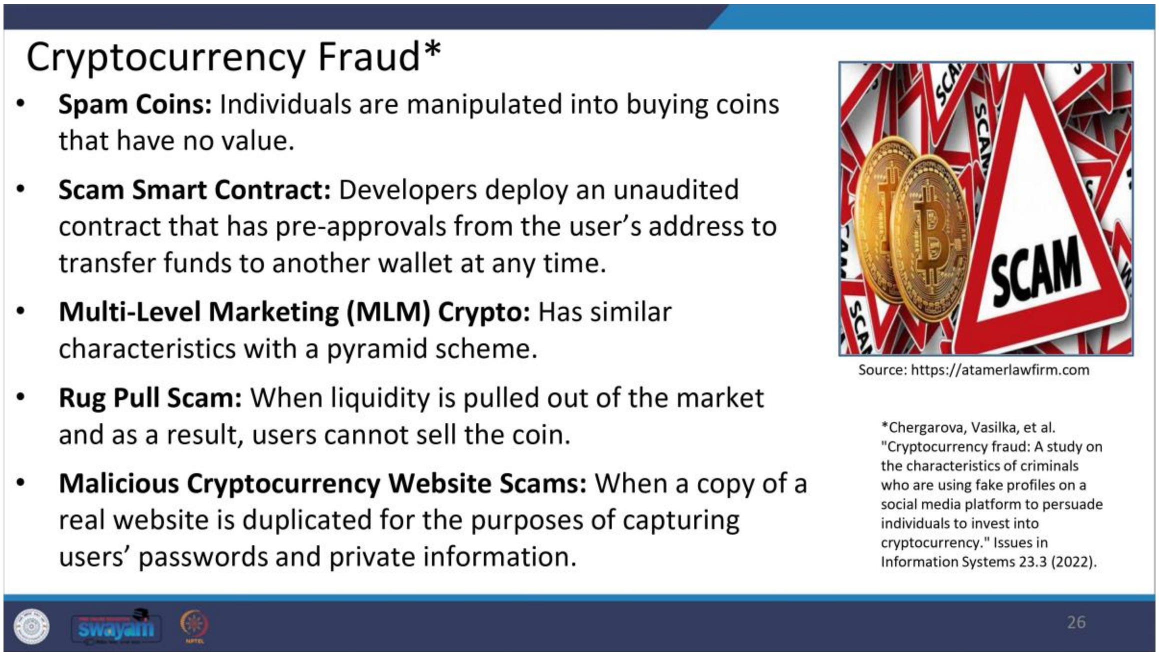
- In pump and dump schemes, scammers artificially inflate the price of a low-value investment through false or misleading information.
- Once the price rises, the scammers sell their shares, causing the price to plummet, leaving other investors with substantial losses.
  - The Wolf of Wall Street: Jordan Belfort, the subject of the book and movie "The Wolf of Wall Street," operated a pump and dump scheme through his brokerage firm, Stratton Oakmont
  - The company manipulated stock prices, creating a frenzy of buying before selling off their shares at inflated prices.

Leonardo DiCaprio as Jordan Belfort in *Wolf of the Wall Street* (2013)
Source: https://wifflegif.com

*Weiner, Pierre M., Robert D. Weber, and Kirby Hsu. "The growing menace of 'short and distort'campaigns." *Westlaw Journal Securities Litigation & Regulation* 31 (2017).

In pump and dump schemes, scammers artificially inflate the price of a low value investment through falls or misleading information. Once the price rises, the scammers sell their shares causing the price to plummet leaving other investors with substantial losses. We can refer to the famous book and movie The Wolf of Wall Street in which Jordan Belfort operated a pump and dump scheme through his brokerage firm. The company manipulated stock prices creating a frenzy of buying before selling of their shares at inflated price.

This investment scams often entice individuals with promises of high returns and low risk exploiting their desire for financial gain. And therefore, it is important to conduct a thorough research and practice due diligence before making any investment decisions. More recently, cryptocurrency fraud seems to be on the rise which follows the same principles as pyramid schemes.



Cryptocurrency Fraud*

- **Spam Coins:** Individuals are manipulated into buying coins that have no value.
- **Scam Smart Contract:** Developers deploy an unaudited contract that has pre-approvals from the user's address to transfer funds to another wallet at any time.
- **Multi-Level Marketing (MLM) Crypto:** Has similar characteristics with a pyramid scheme.
- **Rug Pull Scam:** When liquidity is pulled out of the market and as a result, users cannot sell the coin.
- **Malicious Cryptocurrency Website Scams:** When a copy of a real website is duplicated for the purposes of capturing users' passwords and private information.

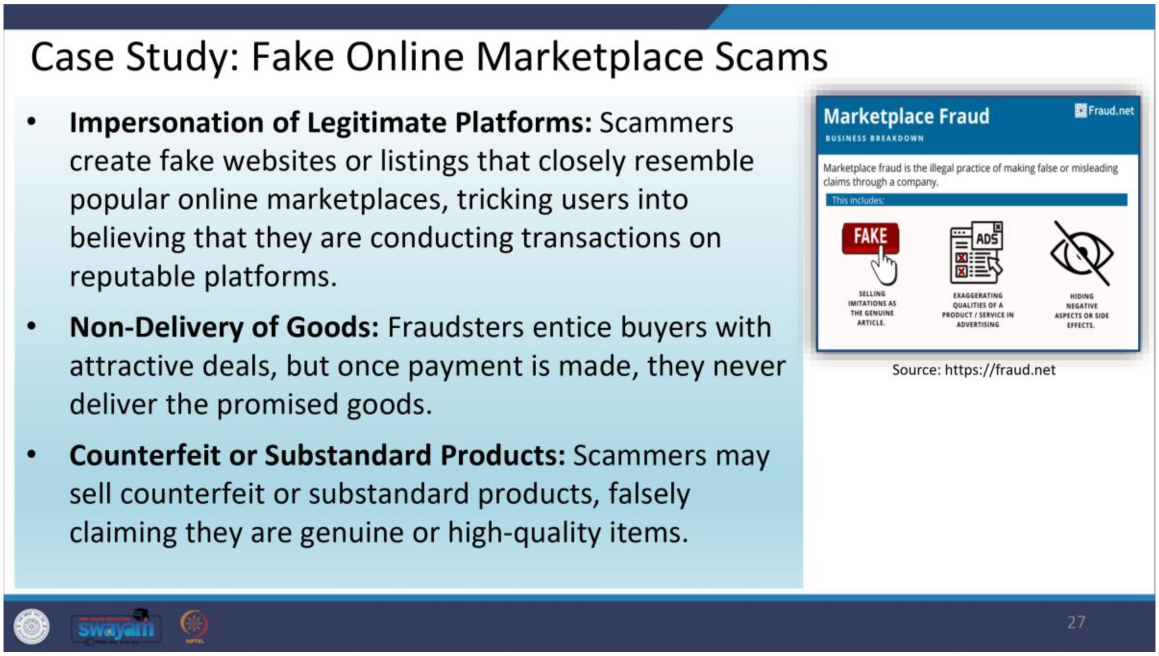
Source: https://atamerlawfirm.com

*Chergarova, Vasilka, et al. "Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency." Issues in Information Systems 23.3 (2022).

Individuals are manipulated into buying coins that have no real value in fact. Users deploy an unaudited contract that has pre-approvals from the user's address to transfer funds to another wallet at any time. There is a multilevel marketing crypto or MLM. It has similar characteristics with a pyramid scheme. There is a rug pull scam also where liquidity is pulled out of the market and as a result users cannot sell the coin. Similarly, when a copy of a real website is duplicated for the purpose of capturing users password and private information, it is named as malicious cryptocurrency website scams.

Additionally, as cryptocurrency uses blockchain for verification and does not run through financial institutions, it is harder to recover from theft. It has also been not legally allowed in various countries. Individuals must be wary of investment opportunities that promise guaranteed high returns or minimal risks or not supported by any regulated financial institution as these claims are often indicators of fraudulent schemes. They should also seek advice from reputable financial professionals to verify the legitimacy of investment opportunities.

Let us now take a look at some real world case studies to put this information into perspective. Our first case study deals with fake online marketplace scam that involves fraudsters creating deceptive platforms that may make legitimate online marketplaces.



Case Study: Fake Online Marketplace Scams

- **Impersonation of Legitimate Platforms:** Scammers create fake websites or listings that closely resemble popular online marketplaces, tricking users into believing that they are conducting transactions on reputable platforms.
- **Non-Delivery of Goods:** Fraudsters entice buyers with attractive deals, but once payment is made, they never deliver the promised goods.
- **Counterfeit or Substandard Products:** Scammers may sell counterfeit or substandard products, falsely claiming they are genuine or high-quality items.

Marketplace Fraud

BUSINESS BREAKDOWN

Fraud.net

Marketplace fraud is the illegal practice of making false or misleading claims through a company.

This includes:

SELLING IMITATIONS AS THE GENUINE ARTICLE.

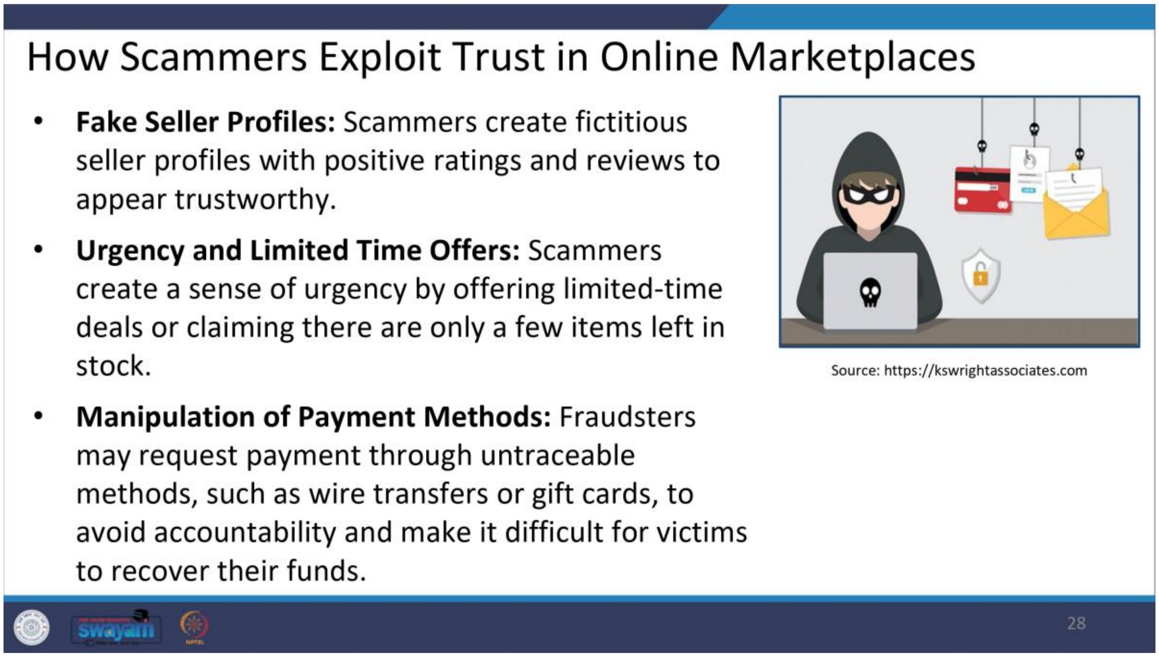
EXAGGERATING QUALITIES OF A PRODUCT / SERVICE IN ADVERTISING

HIDING NEGATIVE ASPECTS OR SIDE EFFECTS.

Source: https://fraud.net

The impersonation of legitimate platforms tricks users into believing that they are conducting transactions on reputable platforms. Fraudsters entice buyers with attractive deals but once payment is made they never deliver the promised good. They also use counterfeit or substandard products falsely claiming that they are genuine or high quality items.

Scammers thus exploit the trust established in online marketplaces to deceive buyers as well as sellers.



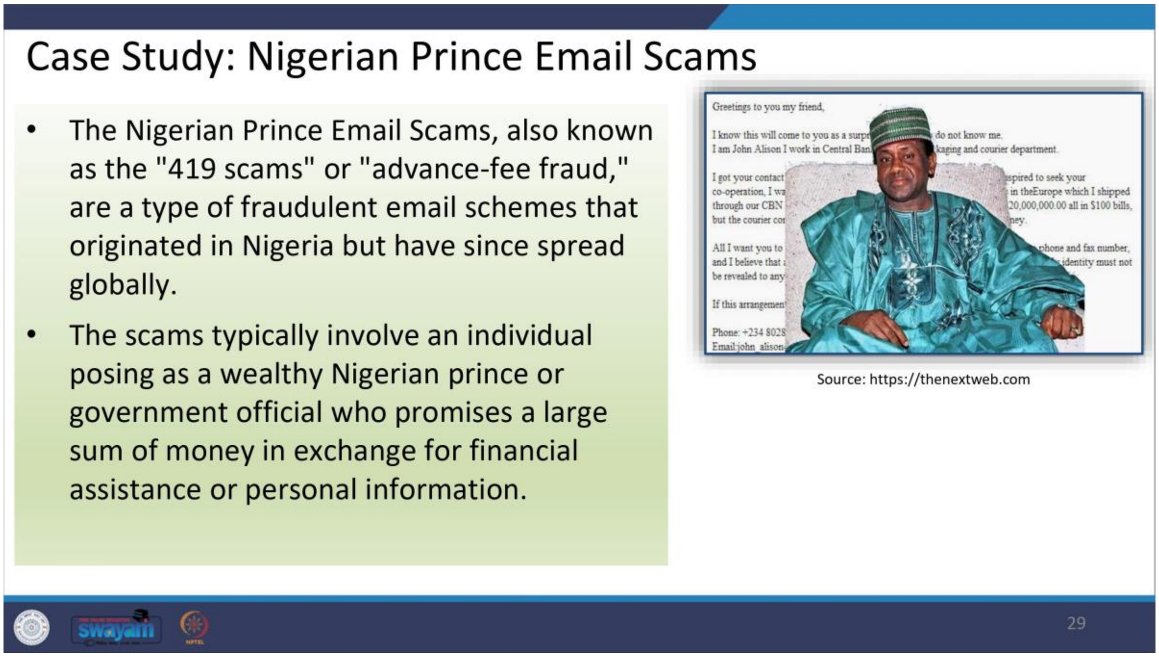
How Scammers Exploit Trust in Online Marketplaces

- **Fake Seller Profiles:** Scammers create fictitious seller profiles with positive ratings and reviews to appear trustworthy.
- **Urgency and Limited Time Offers:** Scammers create a sense of urgency by offering limited-time deals or claiming there are only a few items left in stock.
- **Manipulation of Payment Methods:** Fraudsters may request payment through untraceable methods, such as wire transfers or gift cards, to avoid accountability and make it difficult for victims to recover their funds.

Source: https://kswrightassociates.com

So how do scammers exploit trust in online marketplaces? Firstly, they may create fake seller profiles with positive ratings and reviews in order to come across as trustworthy. They also create a sense of urgency by offering limited time deals or claiming that only a few items are now left. They also manipulate the payment methods and they may request payments through untraceable methods such as wire transfers or gift cards to avoid accountability and make it difficult for victims to recover their funds. It also makes it difficult for the law enforcement agencies to trace such financial transactions.

Fake proactive measures when engaging in online transactions can help us in safeguarding against fake online marketplaces scams and protect our financial well-being. For our second case study, we will look into the Nigerian Prince email scams which are a common form of online fraud. Scammers impersonate wealthy individuals seeking or providing financial assistance.

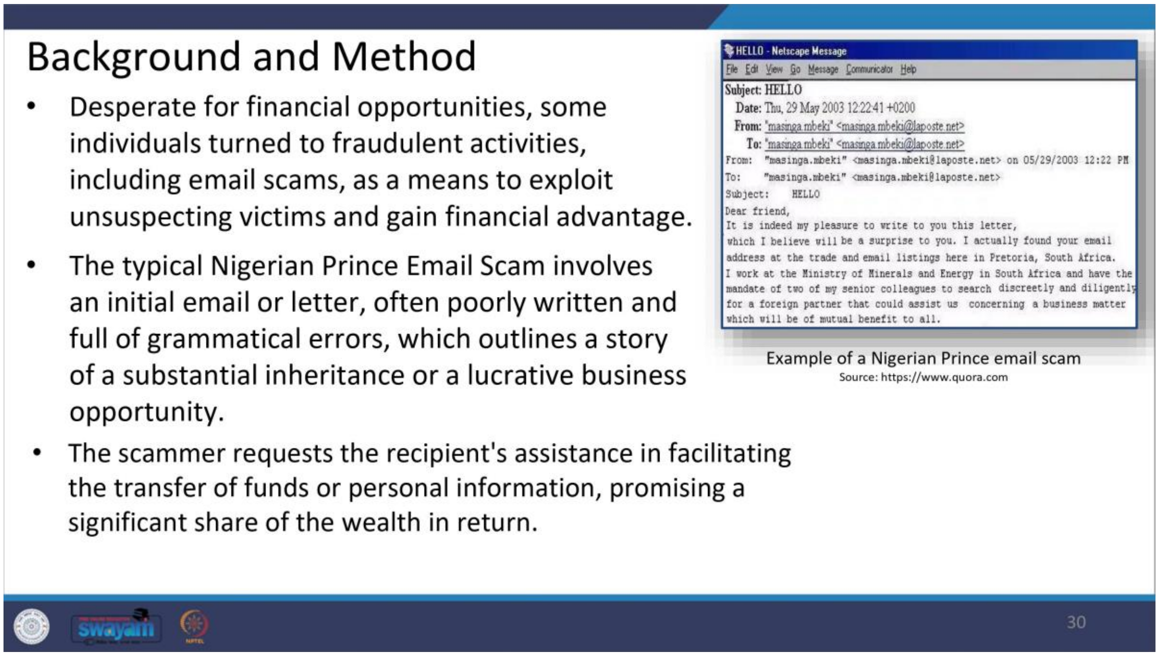


Case Study: Nigerian Prince Email Scams

- The Nigerian Prince Email Scams, also known as the "419 scams" or "advance-fee fraud," are a type of fraudulent email schemes that originated in Nigeria but have since spread globally.
- The scams typically involve an individual posing as a wealthy Nigerian prince or government official who promises a large sum of money in exchange for financial assistance or personal information.

Source: https://thenextweb.com

The Nigerian Prince email scams also known as the 419 scams or advance free fraud are a type of fraudulent email schemes that originated in Nigeria but have since spread globally. The scams typically involve an individual posing as a wealthy Nigerian Prince or government officials who promises a large sum of money in exchange for financial assistance or personal information. The background of these scams can be traced back to the 1980s when Nigeria faced economic challenges and political instability. Disparate for financial opportunities, some individuals turn to fraudulent activities including such email scams to financially exploit unsuspecting victims.



Background and Method

- Desperate for financial opportunities, some individuals turned to fraudulent activities, including email scams, as a means to exploit unsuspecting victims and gain financial advantage.
- The typical Nigerian Prince Email Scam involves an initial email or letter, often poorly written and full of grammatical errors, which outlines a story of a substantial inheritance or a lucrative business opportunity.
- The scammer requests the recipient's assistance in facilitating the transfer of funds or personal information, promising a significant share of the wealth in return.

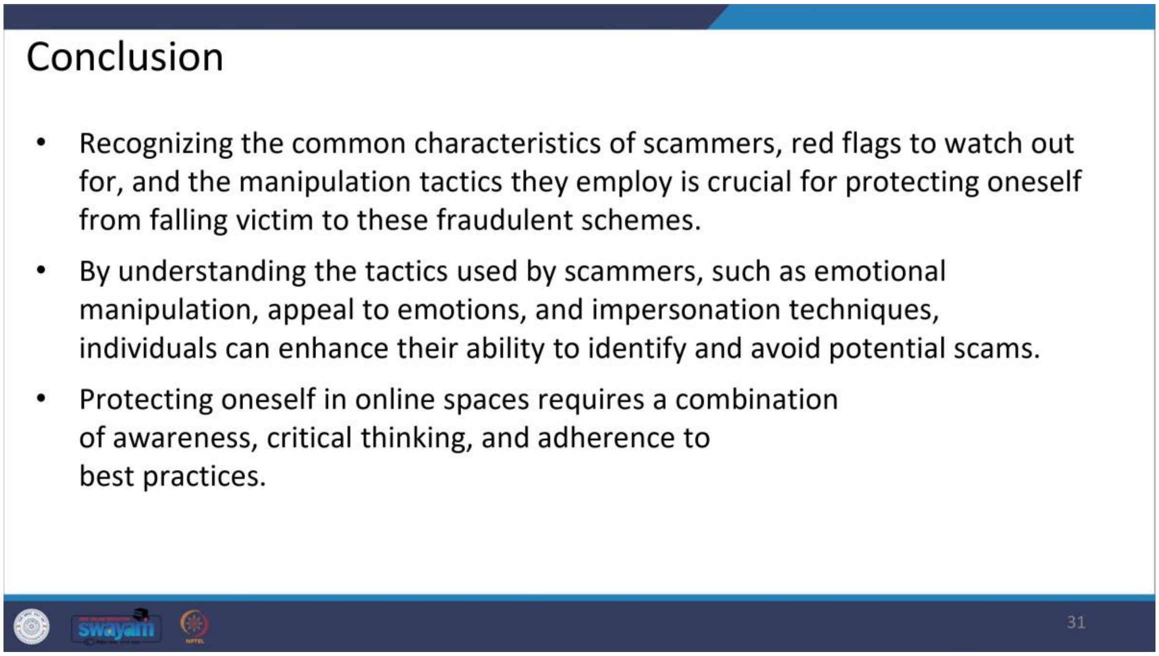
```
Subject: HELLO
   Date: Thu, 29 May 2003 12:22:41 +0200
   From: "masinga mbeki" <masinga mbeki@laposte.net>
     To: "masinga mbeki" <masinga mbeki@laposte.net>
From:  "masinga.mbeki" <masinga.mbeki@laposte.net> on 05/29/2003 12:22 PM
To:    "masinga.mbeki" <masinga.mbeki@laposte.net>
Subject:    HELLO
Dear friend,
It is indeed my pleasure to write to you this letter,
which I believe will be a surprise to you. I actually found your email
address at the trade and email listings here in Pretoria, South Africa.
I work at the Ministry of Minerals and Energy in South Africa and have the
mandate of two of my senior colleagues to search discreetly and diligently
for a foreign partner that could assist us  concerning  a business matter
which will be of mutual benefit to all.
```

Example of a Nigerian Prince email scam
Source: https://www.quora.com

The typical Nigerian Prince email scam involves an initial email or letter often poorly written and full of grammatical errors which outlines a story of a substantial inheritance or a lucrative business opportunity. The scammer requests the assistance from the recipient in order to facilitate the transfer of funds or personal information promising a significant share of the wealth in return.

Over the years, these scams have become more sophisticated with scammers using various tactics to deceive victims. They often impersonate legitimate individuals or organizations, create fake websites or use social engineering techniques to gain the trust of their targets. The Nigerian Prince email scams have become notorious and have affected individuals, businesses and even sometimes some governments worldwide. These scams serve as a reminder to exercise caution and skepticism when receiving unsolicited emails or request for personal or financial information.

In conclusion, online scams and swindlers in online communication and spaces pose significant risk to individuals' financial and emotional wellbeing, personal information and overall security.



Conclusion

- Recognizing the common characteristics of scammers, red flags to watch out for, and the manipulation tactics they employ is crucial for protecting oneself from falling victim to these fraudulent schemes.
- By understanding the tactics used by scammers, such as emotional manipulation, appeal to emotions, and impersonation techniques, individuals can enhance their ability to identify and avoid potential scams.
- Protecting oneself in online spaces requires a combination of awareness, critical thinking, and adherence to best practices.

So, it can be said that recognizing the common characters of scammers, red flags to watch out for and the manipulation tactics they employ is crucial for protecting oneself from falling victim to such fraudulent schemes. By understanding the tactics used by scammers such as emotional manipulation, appeal to emotions and sentiments and impersonation techniques, individuals can enhance their ability to identify and avoid potential scams. Protecting oneself in online spaces requires a combination of awareness, critical thinking and adherence to best practices. Additionally, being aware of different types of scams empowers individuals to take informed decisions and take proactive measures to protect themselves.

By staying informed, remaining vigilant and practicing safe online practices, we can minimize our vulnerabilities. Digital communication as we have seen comes with certain dangers, but as they say prevention is better than cure. We will discuss some other aspects of digital communication in the next module. Thank you.