Social Engineering

https://www.youtube.com/watch?v=9q4j7GtS4OI

Who are Hackers/Crackers or Ethical Hackers?


addresses
socials
emails
credit cards
passwords
birthdays
ФЙЖ

The Easiest Way of Hacking?

The easiest way to break into any computer system is to use a valid username and password and the easiest way to get that information is to ask someone for it.

Vishing/ Smishing

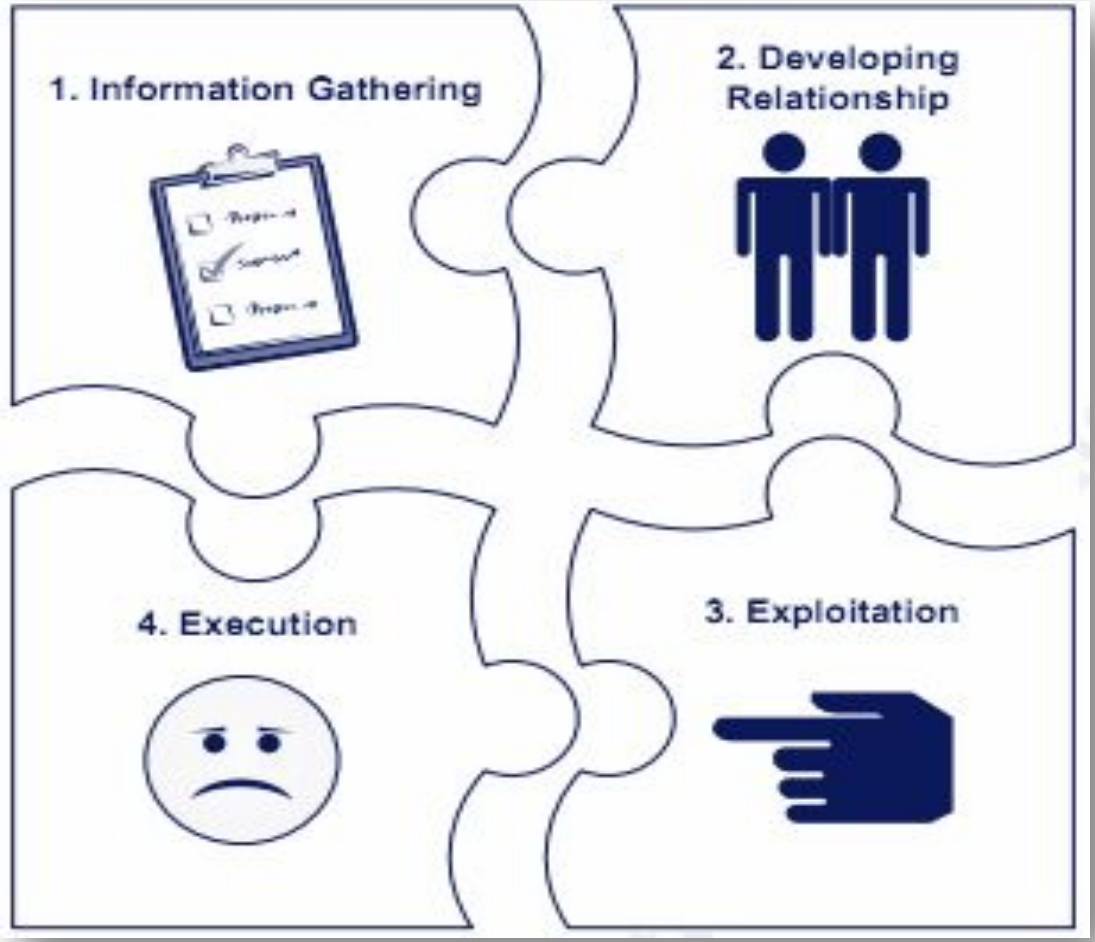
What is Social Engineering

Who can be Social Engineers

- Hackers
- Penetration Testers
- Spies / Espionage
- Identity Thieves
- Disgruntled Employees
- Information Brokers
- Scam Artists
- Executive Recruiters
- Sales People
- Everyday People

Social Engineering

How it works



Social Engineering Attacks

- Phone
- Phishing
- Vishing
- Whaling
- Spear Phishing
- Delivery
- Dating & Love
- Tech Support
- Goods Delivery
- Nigerian 419
- Credit Card Block
- Celebrity
- Lottery
- VOIP

WHY SOCIAL ENGINEERING?

HACKING A HUMAN IS **MUCH EASIER** THAN HACKING A BUSINESS.

"Social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest."

- Christopher Hadnagy, Unmasking the Social Engineer, 2014 Wiley

People are usually the **weakest** link in a security chain, and most human error is attributed to lack of security knowledge, lack of training, or a failure to follow security procedures.

294

Billion emails are sent per day, that's

2.8 million emails every second.

90% Of these messages are spam.

19%

of all emails delivered to corporate inboxes are spam, despite spam filters.

Most computers use anti-virus software, yet many are still hit by viruses and worms.

For the subject line, spammers are doing **everything in their power to** make the recipient click and open the message.

Top 6 Spam Categories

1.	Dating	19%
2.	Pharmeceuticals	16%
3.	Malware	12%
4.	Gambling	3%
5.	Replicas	1%
6.	Adult	1%

90%

of data breaches could have been prevented

3 BASIC TYPES OF TACTICS

Cyber Stalking

CyberStalking is the use of Internet and/or other electronic communication devices to stalk another person.

It involves harassing or threatening behaviour that an individual will conduct repeatedly.

For example following a person, making phone calls, sending vulgar emails etc

Cyber Bullying

Offesive messages or Images are posted or send to harass or embrace others

Phishing

Tue 29/12/2015 17:11

PayPal <confirmagain@ppservice.com>

Your PayPal account has been limited

To [redacted]

PayPal

Update Required!!

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity.

This is part of our security process and helps ensure that PayPal continue to be safer way to buy online. Often all we need is a bit more information. While your account is limited, some options in your account won't be available.

How to remove my limitation?

You can resolve your limitation by following these simple steps:

- **Log in here**.
- Provide the information needed. The sooner your provide the information we need, the sooner we can resolve the situation.

"If this message sent as Junk or Spam, its just an error by our new system, please click at Not Junk or Not Spam"

Sincerely,

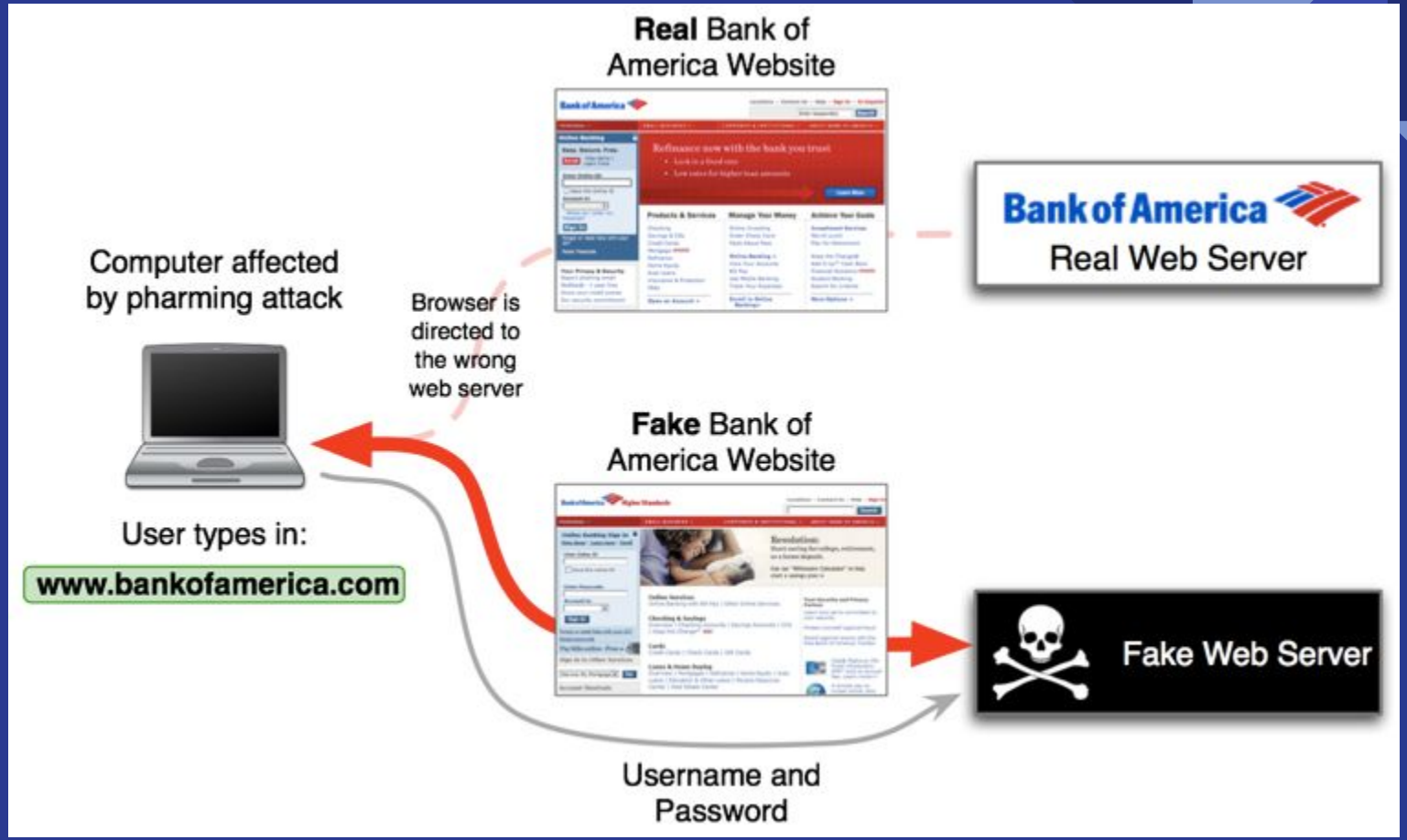
PayPal


Fake address bar covers the real one
PayPal
Member Log In
Lock icon does not appear in the browser status bar

Pharming

Misdirecting users to fraudalent websites


Google Search: westpac - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?client=firefox-a
Go
Google
Web Images Groups News Froogle Local more »
westpac
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 1,300,000 for westpac. (0.13 seconds)
https://olb.westpac.com.au/
3k - 14 Jul 2005 - Cached - Similar pages
Westpac New Zealand
Westpac New Zealand provides online banking, everyday transaction accounts, loans, credit cards, foreign exchange, insurance, and savings and investment ...
www.westpac.co.nz/olcontent/olcontent.nsf/Content/Personal_HomePage - 18k - Cached - Similar pages
Sponsored Links
FOREX Secrets
Information On FOREX Trading - Guidelines, Tips & Resources.
com-go.com/forex.html
Westpac New Zealand Choices home loan rates
Westpac's current interest rates as at 15 July 2005. Want to know more about our fixed, ... Westpac banking package interest rate discounts do not apply. ...
www.westpac.co.nz/olcontent/ olcontent.nsf/Content/Choices+home+loan+rates - 18k - 14 Jul 2005 - Cached - Similar pages
[More results from www.westpac.co.nz]
Done


Real Bank of America Website
Bank of America
Real Web Server
Computer affected by pharming attack
Browser is directed to the wrong web server
Fake Bank of America Website
User types in:
www.bankofamerica.com
Fake Web Server
Username and Password

MODUS OPERANDI

STEP 1

Culprit makes phone call posing as bank executive for card upgrade

STEP 2

Victim questions authenticity of the caller

Culprit initiates purchase using card details

3 STEP

4

Bank sends OTP to victim's phone which culprit claims as proof

Culprit makes the victim share OTP to complete fradulent purchases

5 STEP

Delivery Attack

- Target is a “winner” of an expensive / attractive product being offered free of cost
- Only Delivery Charge has to be paid and will be collected in cash at the doorstep against delivery
- A “delivery man” will bring a package that is delivered on payment of a Delivery Charge
- The package will be empty or will have some worthless material

Dating & Love – Target Lonely Hearts

- Imposter will befriend them on Facebook or Social Media or Matrimonial sites
- The target receives a call from a “Customs Officer” with a demand for payment of customs duty payable for a gift parcel.
- This ‘gift’ has been sent by the boyfriend who wanted to surprise his beautiful love and he is so “sorry” for creating trouble for her, and that he will repay the amount when he comes over to be with her soon
- The target pays the duty amount **which is lost**

Love, Dating, Marriage Attacks

Printed from
THE TIMES OF INDIA

45-year-old woman duped of Rs 1.2 crore in matrimonial site fraud over 15 months

TNN | Feb 11, 2016, 11.35 PM IST

Representative image.

Kalyan: A 45-year-old Dombivli woman recently approached the Thane cyber police cell alleging she was duped of Rs 1.2 crore by a US resident whom she had befriended on a matrimonial website, and by as many as 36 of his associates, over a span of 15 months.

The main accused introduced himself as a Los Angeles-based

Conmen posing as 'Mr. Right' dupe Mumbai women of their savings

By Vijay Kumar Yadav | Posted 08-May-2016

In a Ladies Vs Ricky Bahl moment, nine city women connect over married man with modest Railways job who posed as Bandra pilot to plunder their savings. The do-or-die battle to land Mr Right is costing young women big bucks

Hong Kong police bust transnational love scam that duped wo…
www.scmp.com › News › Hong Kong › Law & Crime
Dec 16, 2016 - In an unprecedented joint operation, Hong Kong, Malaysian and Nigerian police have busted a syndicate running **online** romance scams which ...

'I was scammed by an online love rat too' - News.com.au
www.news.com.au/...**online-love**...**internet**.../0ed4d0101ccc67654b9811...
Jul 2, 2015 - 'I was scammed by an **online love** rat too,' survivors of **internet** fraud speak out ... “A few days later I got a call from a **woman** who said she was his lawyer, ... number of Australians **tricked by online** romance scams and frauds.

Woman, 58, believes she was duped out of £50000 by bigami…
www.dailymail.co.uk/.../**Woman**-58-reveals-**duped**-50-000-bigamist-**lov**...
Mar 11, 2015 - **Woman**, 58, believes she was **duped** out of £50,000 by bigamist **love** rat who was ... Kim Sow reveals all on her bigamist **love** rat husband ..... before slipping into a slinky gold two-piece during **Indian** getaway

BAITING – using USB, Free music, Files

- Baiting promises an item or goods to entice victims.
    - Free music or movie downloads (if they submit their login credentials)
    - Files
- Attacks can exploit human curiosity in real life
    - USB Attack
        - Infected USBs with a Trojan virus are dispersed around the parking lot.
        - Employees may pick up the USBs and plug them into their computers, activating a keylogger

Hack The Human

- CEO was brought to ruin through a charity scam:
  - Social engineers found out he had a family member who was battling cancer and other information through his Facebook page.
  - Using that emotional attachment, they tugged at his heartstrings and he was asked to donate money to a cancer research fund.
  - The PDF that was sent, however, was malware that took control of his computer
- Happy family enters a theme park and discovers that they forgot to carry a printout of the entry coupon!
  - Appealing to the human nature of the ticket booth, they ask the workers if they may bring up the email file and print out the coupon, or even just to show that they indeed have a coupon.
  - Unfortunately, that harmless family is a group of actors looking to get in the park's system by bringing up a harmful file on their computers.

Credit Card Block / Entitlement

- Email / Phone saying your card is blocked or will be blocked
- URL / Phone number is provided for sharing information
- Target will provide the existing card information
- Target is prompted for PIN / OTP
- Card is misused for payments by scamster

Nigerian Scam

https://classroom.google.com/g/tg/MjcyNDkyODQzMjRa/MzI2ODM2MDIyMjJa#u=NDYxNDI1OTgxOVpa&t=f

Social Engineering Cases / Examples

Robin Sage

From Wikipedia, the free encyclopedia

For the military training exercise, see United States Army Special Forces selection and training.

Robin Sage is a fictional American cyber threat analyst. She was created in December 2009 by Thomas Ryan, a controversial security specialist and white hat hacker from New York City. Her name was taken from a training exercise of United States Army Special Forces.[1]

"Robin Sage" as she appeared on social networking pages.

Contents [hide]

Fictional biography [edit]

According to Sage's social networking profiles, she is a 25-year-old "cyber threat analyst" at the Naval Network Warfare Command in Norfolk, Virginia. She graduated from MIT and had allegedly 10 years of work experience, despite her young age.[2] Ryan created several accounts under the name Sage on popular social networks like Facebook, LinkedIn, Twitter etc. and used those profiles to contact nearly 300 people, most of them security specialists, military personnel, staff at intelligence agencies and defense contractors.[1] Her pictures were taken from a pornography-related website in order to attract more attention.[2]

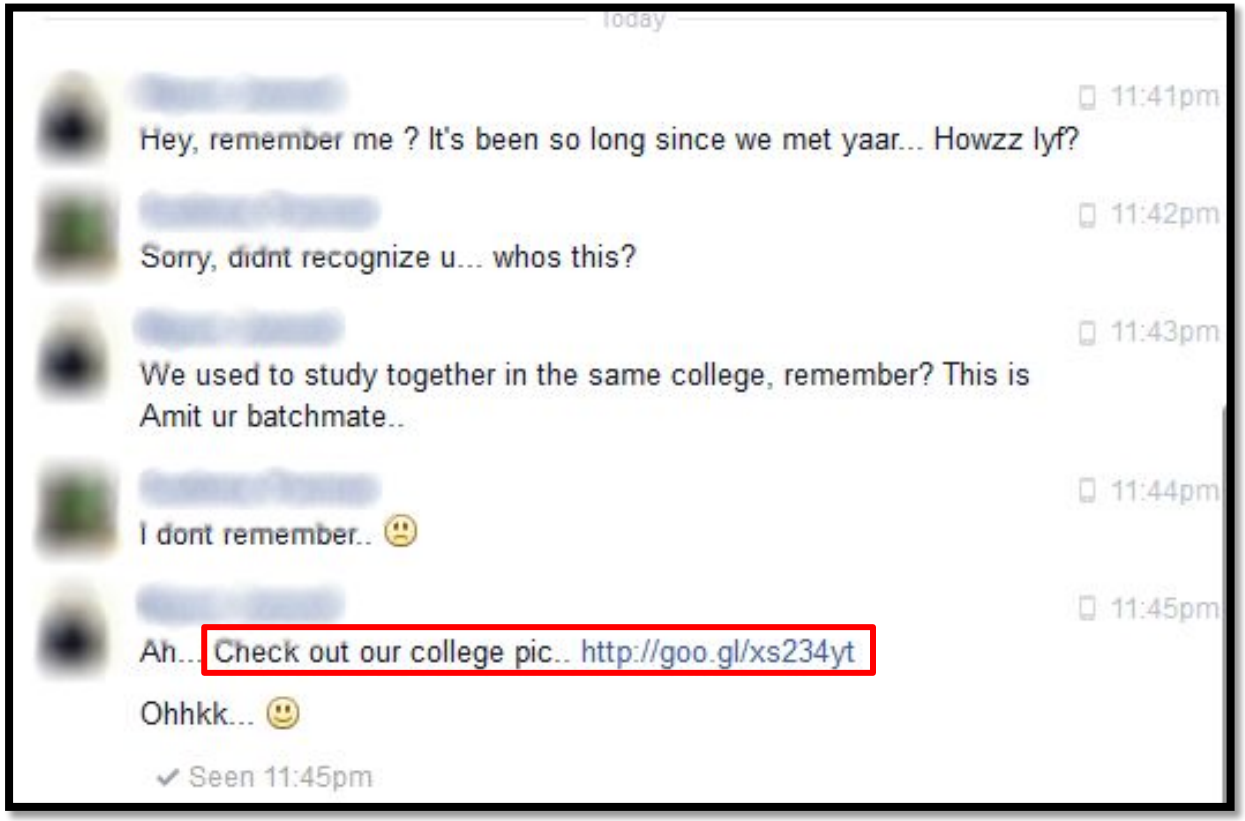
Robin Sage's saga

25-year-old "cyber threat analyst" at the Naval Network Warfare Command in Norfolk, Virginia. MIT graduate; 10 years of work experience!

- Sage was offered consulting work with notable companies Google and Lockheed Martin and received dinner invitations by several of her male friends.
- Security problems revealed
- Using those contacts, Ryan befriended men and women of all ages during a short time period
- Between December 2009 and January 2010 made friends and almost all were working for US military, government or companies and gained access to email addresses, bank accounts as well as learning the location of secret military units based on soldiers'
- She was also given private documents for review and was offered to speak at several conferences
- The experiment proved
  - seemingly harmless details shared via social networking pages can be harmful
  - also that many people entrusted with vital and sensitive information would share this information readily with third parties, provided they managed to capture their interest.
  - could have compromised national security if a terrorist organization had employed similar tactics.

"Robin Sage" as she appeared on social networking pages.

Chatting going wrong



Another officer duped in credit card fraud

Lucknow: With credit card frauds on the rise in the Uttar Pradesh Capital, yet another senior IAS official has been duped.

Mr P L Loi, posted as Principal Secretary Science and Technology, was duped by two impersonators posing as representatives of the ICICI bank.

He lodged an FIR with the Gomti Nagar police on Sunday claiming the duo took his credit card with a promise to upgrade it without any additional fee.

One of the young men introduced himself as Shobhit Baghel and started a discussion on credit cards. During the course of discussion, he checked on Mr. Loi's credit card and advised him to get his card renewed. An unsuspecting official fell for the trap.

On Saturday, the bank informed Mr. Loi that about Rs 40,774 had been withdrawn from his account. He ordered his account be frozen immediately and later informed the police.

This is the second time an IAS officer had been cheated through credit card.

Earlier, another senior IAS officer Rohit Nandan found his ATM account hacked and a substantial sum withdrawn.

50 IAF officers fall victim to credit card fraud

Investigators are probing the role of some insiders and are planning to grill SBI officials and also IAF personnel.

Mail Today Bureau New Delhi, July 25, 2014 | UPDATED 15:38 IST

More than 50 officials, including senior officials, of the Indian Air Force have become the latest victims of credit card fraud.

The Air Force has registered an FIR with the Cyber Cell of Delhi Police in connection with over 50 cases of fraudulent withdrawal of money from State Bank of India (SBI) accounts of its air force officers posted across India. Investigators are probing the role of some insiders and are planning to grill SBI officials and also IAF personnel.

A senior police officer said the IAF had shifted bulk of its officers' bank accounts to the SBI in 2009-10 and most of the affected customers are from Defence Salary Package, a large number of them from the Air Force. The case was registered on Wednesday evening following the complaint of the Commanding Officer of IAF's Provost and Security Unit, Wing Commander Tejveer Singh. "We came to know that our Air Force officials had lodged complaints with the local police," said Singh.

Case Studies

Social media thefts on rise in the city: Unmarried youngsters most vulnerable

Vinita Chaturvedi Jan 13, 2017, 08.11 PM IST

the family, cops or the society at large.

Rising menace

In almost all the recent cases registered i
promise of love and marriage and later a
youngsters were made to deposit large a
different banks via netbanking. And once
lovers, whom the victims met on faceboo
cases has increased considerably in the p

Slick modus operandi

One such case was registered recently at
same police station Satyaveer Bandiwar
modus operandi. They make fake accoun
cities. And these fraudsters carry out diffe
places. For example, calls are made from
transferred to Nigeria. So, it is difficult to

Every trick in the (Face)book: Scammers use social media to swindle money, target younger victims

By Kelsey Price on Jan 26, 2017 at 2:00 p.m.

Scammers just keep getting trickier. With social media, it's possible to be hacked through fake profiles as well as other tactics. Meagan Pitsilkis / Forum Ne

DETROIT LAKES, Minn. — Cons and scams have been around since humans first learned how to communicate but, these days, as communication increases with technology, scams are evolving, increasing in magnitude and allowing con artists to work behind a veil.

Their latest mask? Facebook.

A Detroit Lakes resident nearly fell victim to a Facebook scam on Monday, when she received a friend request from her neighbor — which she thought odd, considering she was already Facebook friends with her neighbor.

After accepting the friend request, the "neighbor" began private messaging her to tell her she had won $100,000. All she needed to do was deposit a monetary advance into an account for the prize money to be delivered.

Realizing it was a scam, the woman then contacted her neighbor, and the two took the necessary measures, contacting friends and deleting accounts, to reconcile the situation.

'Social media creating rift in couples'

Santosh Sonawane| TNN | Jan 21, 2017, 11.32 PM IST

A- A+

NASHIK: The recent murder-suicide case of a couple from the city in Pune has triggered a debate, with police and experts admitting that social media is indeed affecting relationships between married couples.

Software professional Rakesh Gangurde, (34) allegedly murdered his wife Sonali (28) and later hanged himself from the ceiling fan at their rented house in Manjri Budruk, around 12km from Pune, on Tuesday night.

A note written by Gangurde said there were frequent arguments between him and his wife over her sharing details with her friends on social networking sites about their marriage and other personal matters.

Senior officials of the Women's Safety Cell of the Nashik police admitted said the incident is a clear indication of the level of anger that simmers within married couples over the addiction of social media when they find their better half engaged for long hours.

"Our cell got 685 applications of quarrels between husband and wife last year and majority of them were related to discord over the use of social media for long hours," assistant police inspector Manisha Kashid of the cell told TOI on Friday.

Initial investigations in many such cases revealed that the use of social media for long hours had led to suspicions of extra-marital affairs, she said

While the complaints were mainly against husbands, there was a good percentage of husbands who complained about their wives as well," said Kashid.

Organisations working for the safety and welfare of women said that they were also receiving many complaints by married couples against the use of social media.

Facebook and Social media as a social engineering platform

- https://blog.avast.com/social-engineering-hacks

Phising Statistics

- https://www.proofpoint.com/us/security-awareness/post/latest-phishing-first-2019

What is the solution?

- Password(use passphrase)
- Two Factor Authentication
- Stay strong Emotionally
- Protect your PII
- Don’t fall prey to offers and discount(Nothing is Free in the Digital world)
- Organisations should conduct regular drills on their employees and trainings
- Proper Security policy in place