MODEL INSTITUTE OF ENGINEERING & TECHNOLOGY

MIET

FUTURE BEGINS HERE....

ENGINEERING SEMINAR PROPOSAL

Cyber Hygiene

Final Evaluation

Presenter

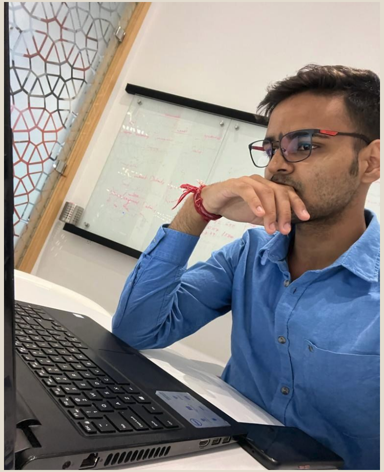
Nihar Zutshi
191203088

Guided by

Mr Arjun Puri

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MIET(Autonomous), JAMMU

About me



Nihar Zutshi
Former Gurugram Cyber Police Summer Intern
4th Year
Department of Computer Science and Engineering,
Model Institute Of Engineering And Technology (Autonomous)

TABLE OF CONTENTS

01 About the seminar

02 What is It?

03 Do & Don’t

04 Data Breach Live Test

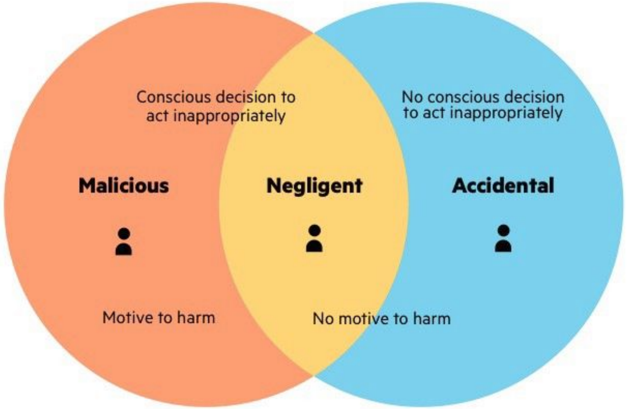
05 Case Study

What is Cybersecurity Hygiene and How do I implement it?

Cybersecurity Hygiene is a set of basic practices that can be taken by all personnel to protect the health of hardware and software of computer-based systems.

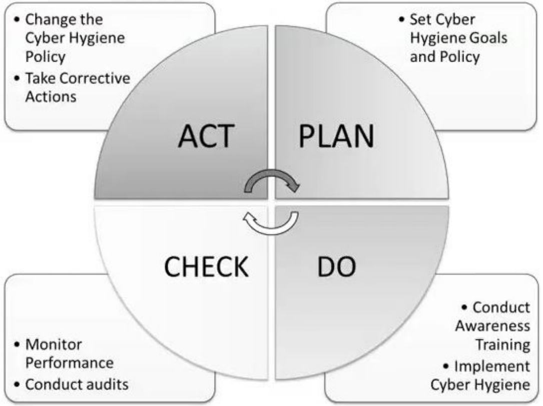
Just as traditional hygiene measures are needed to limit the spread of virus and disease, cybersecurity hygiene is needed to limit the spread of computer viruses and cybersecurity attacks.

The importance of cyber hygiene, cyber hygiene basics, and implementation strategies.


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

Why is cybersecurity Hygiene important for automation systems?

Why is cybersecurity hygiene important for automation systems?


• Change the Cyber Hygiene Policy
• Take Corrective Actions
• Set Cyber Hygiene Goals and Policy
ACT
PLAN
CHECK
DO
• Monitor Performance
• Conduct audits
• Conduct Awareness Training
• Implement Cyber Hygiene

How to Implement Cybersecurity Hygiene?

WHY IS CYBERSECURITY HYGIENE IMPORTANT FOR AUTOMATION SYSTEMS

Why is cybersecurity hygiene important for automation systems?

1. Cyber security incidents can have major consequences for automation systems
2. Cybersecurity risks continue to rise for automation systems
3. the human elements is often the weakest point in security

Cybersecurity risks continue to rise for automation system.

- 90% of OT organizations had experienced a ”damaging attack” in the last two years[1].

- More attackers can target OT systems with readily available hacking tools.

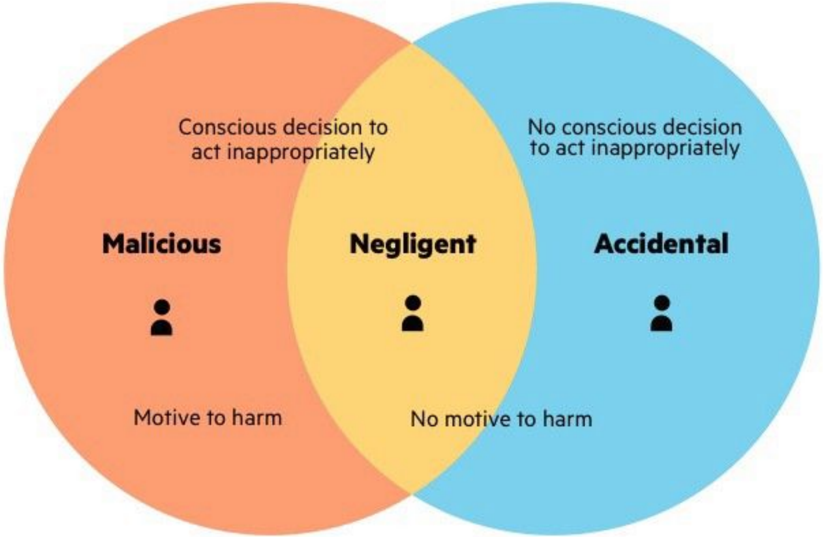
- Aging automation systems often have known vulnerabilities and are no longer patchable.

- Greater interconnectivity and remote access to systems increases possible entry points.

The human elements is often the weakest point in security

1. Nearly 80% of all insider cybersecurity attacks are unintentional 2
   - 64% from employee/contractor negligence
   - 13% from credential theft

2. Many employees (incorrectly) believe their actions have no impact on security


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

WHAT IS CYBERSECURITY HYGIENE?

WHAT IS CYBERSECURITY HYGIENE?

Cybersecurity hygiene is a set of **basic practices** that can be taken by all personnel to protect the health of hardware and software of computer-based systems.

What does cybersecurity hygiene look like?

Awareness of potential sources of cybersecurity risk
- Phishing Emails
- Suspicious Websites
- USB Devices

Following best practices for security
- Using strong unique passwords
- Closing unused accounts
- Maintaining updated devices

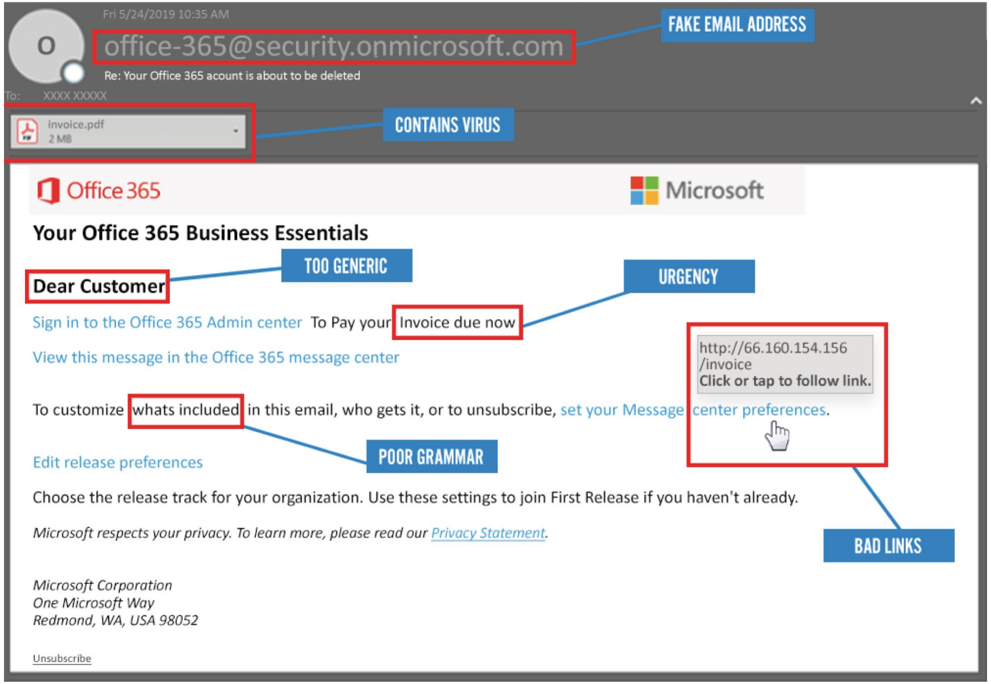
Limiting how much personal information is available online

Phishing is still one of the most used (and effective) methods for compromising user accounts

- Phishing-using email to attempt to acquire sensitive information like passwords, or to tricks users into clicking on a link that downloads malware.
- Without awareness training **37.9%** of employees clicked phishing links
- At large manufacturing companies the number was **48.8%**

These tips can help with detecting a phishing email.

- Be on alert when receiving external links
- Always check the entire email address
- Check for generic greeting
- Be cautious of urgent or demanding actions
- Look for incorrect spelling or grammar
- Check links for secure website



O

Fri 5/24/2019 10:35 AM

office-365@security.onmicrosoft.com

Re: Your Office 365 acount is about to be deleted

To: XXXX XXXXX

invoice.pdf
2 MB

Office 365 — Microsoft

Your Office 365 Business Essentials

Dear Customer

Sign in to the Office 365 Admin center To Pay your Invoice due now

View this message in the Office 365 message center

http://66.160.154.156
/invoice
Click or tap to follow link.

To customize whats included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences

Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

FAKE EMAIL ADDRESS

CONTAINS VIRUS

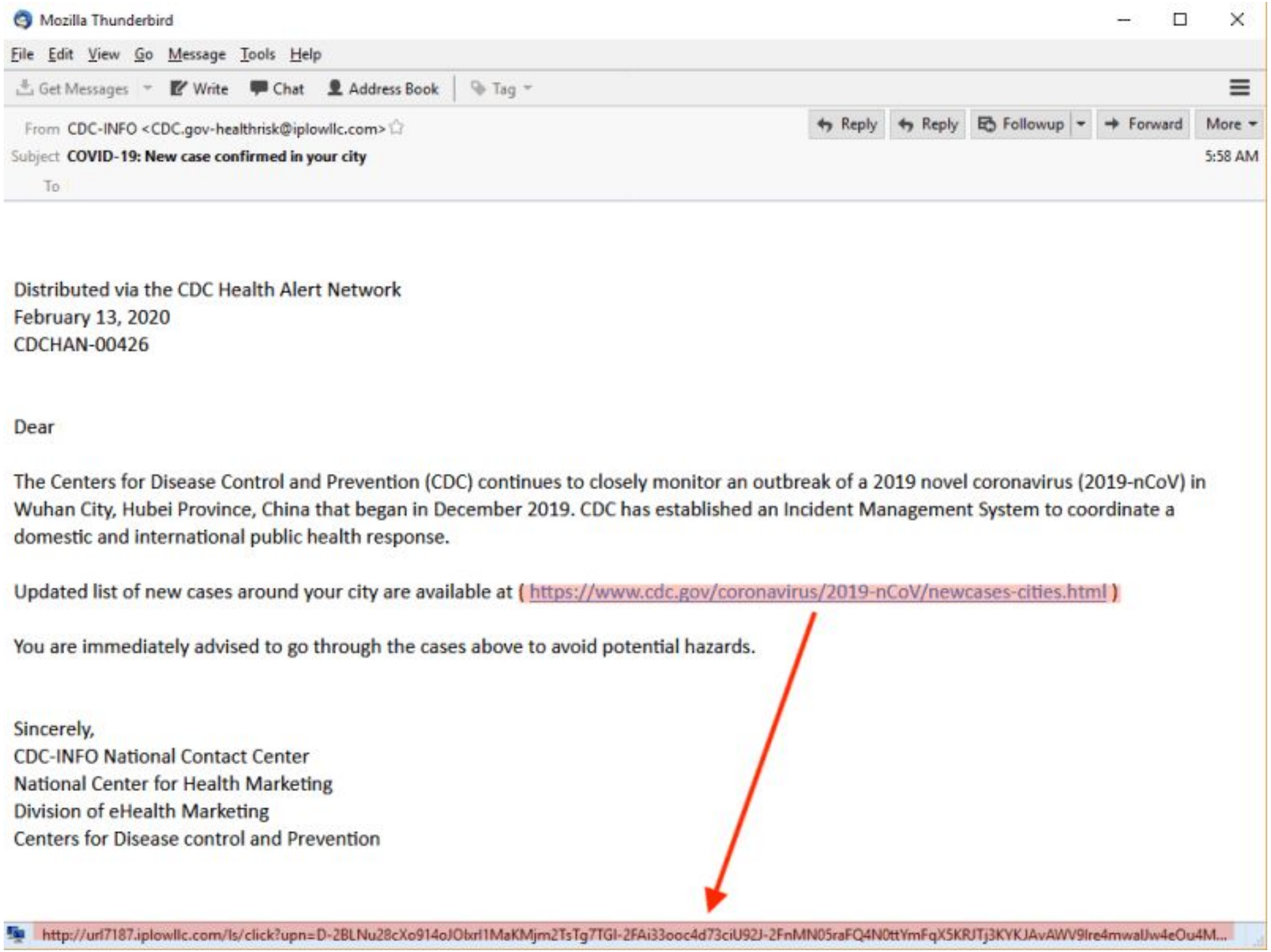
TOO GENERIC

URGENCY

POOR GRAMMAR

BAD LINKS

Reference:-
https://www.newcmi.com/blog/tips-for-detecting-a-phishing-email



From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>

Subject **COVID-19: New case confirmed in your city**

5:58 AM

To

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

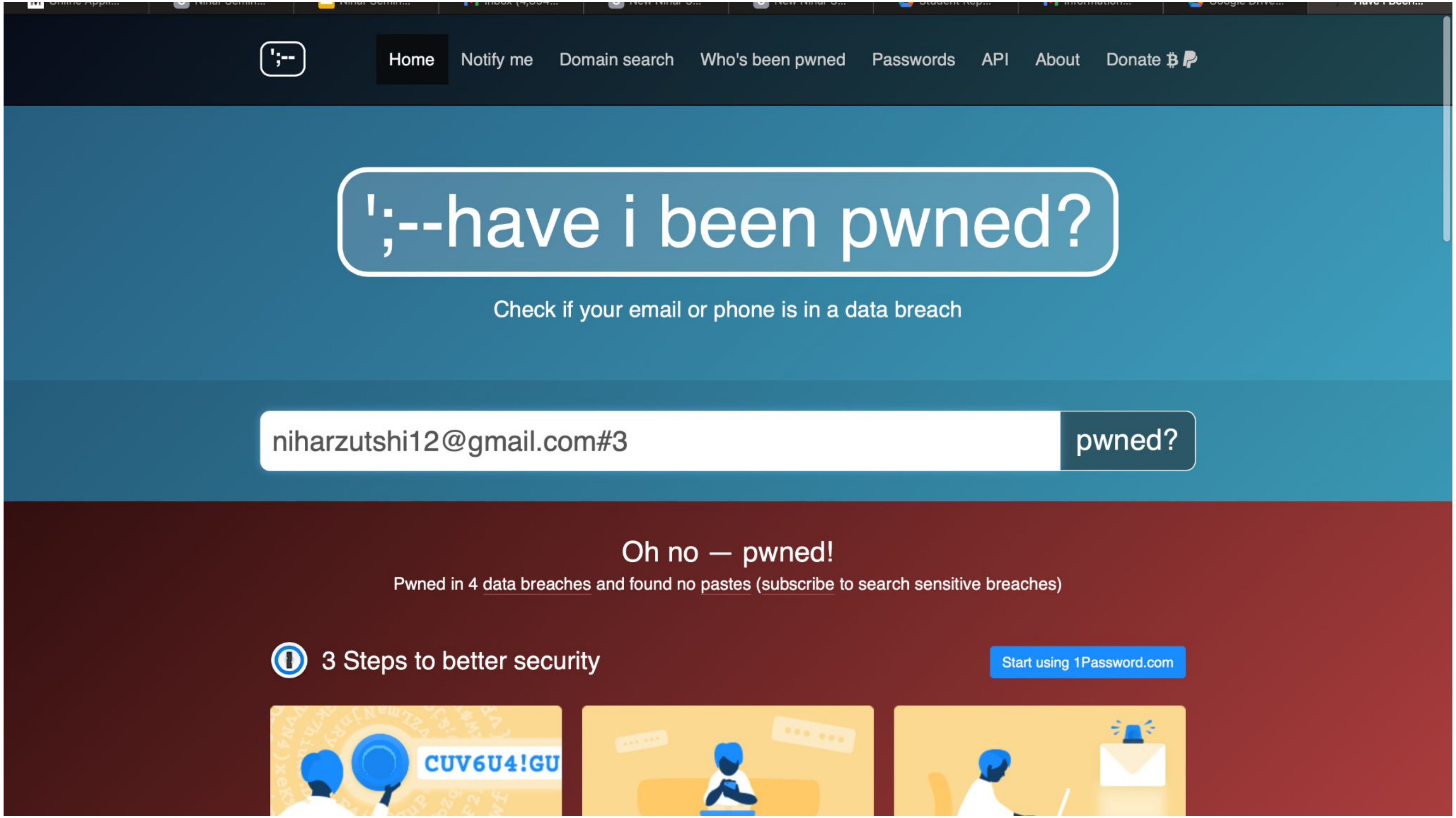
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

http://url7187.iplowllc.com/ls/click?upn=D-2BLNu28cXo914oJObrl1MaKMjm2TsTg7TGI-2FAi33ooc4d73ciU92J-2FnMN05raFQ4N0ttYmFqX5KRJTj3KYKJAvAWV9lre4mwalJw4eOu4M...



';--have i been pwned?

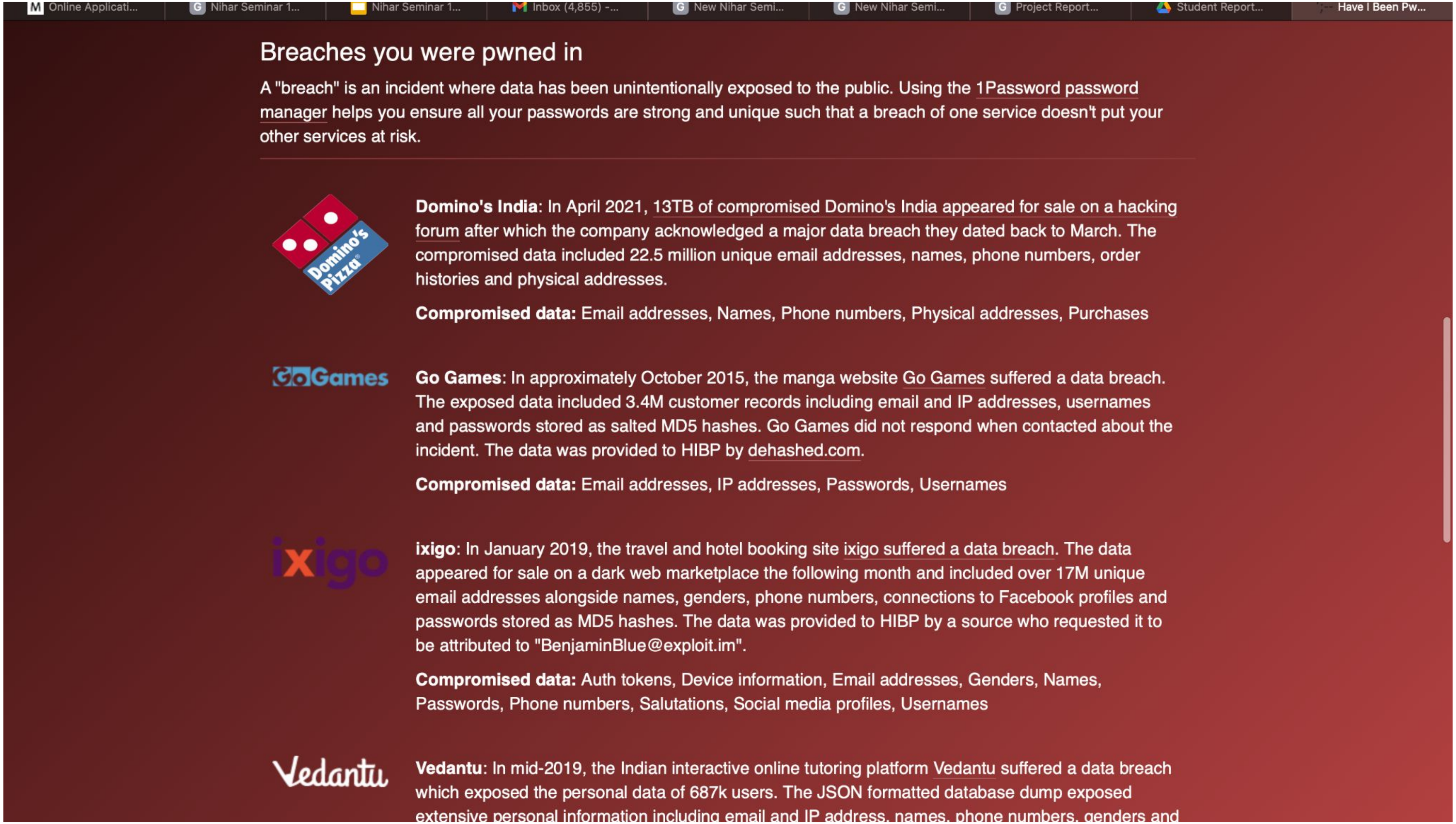
Check if your email or phone is in a data breach

niharzutshi12@gmail.com#3

Oh no — pwned!

Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Domino's India: In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases

Go Games: In approximately October 2015, the manga website Go Games suffered a data breach. The exposed data included 3.4M customer records including email and IP addresses, usernames and passwords stored as salted MD5 hashes. Go Games did not respond when contacted about the incident. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

ixigo: In January 2019, the travel and hotel booking site ixigo suffered a data breach. The data appeared for sale on a dark web marketplace the following month and included over 17M unique email addresses alongside names, genders, phone numbers, connections to Facebook profiles and passwords stored as MD5 hashes. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Auth tokens, Device information, Email addresses, Genders, Names, Passwords, Phone numbers, Salutations, Social media profiles, Usernames

Vedantu: In mid-2019, the Indian interactive online tutoring platform Vedantu suffered a data breach which exposed the personal data of 687k users. The JSON formatted database dump exposed extensive personal information including email and IP address, names, phone numbers, genders and

What Next?

Portable Media is another common source of unintentional malware introduction

- Do not plug in any “found” USBs
- Do not charge cell phones on IACS systems
- Dedicate USBs solely for the use on IACS
- Scan USBs for malware before use

Reference:-
https://www.newcmi.com/blog/tips-for-detecting-a-phishing-email

Following security best practices for all employees can help limit cybersecurity exposure.

DO

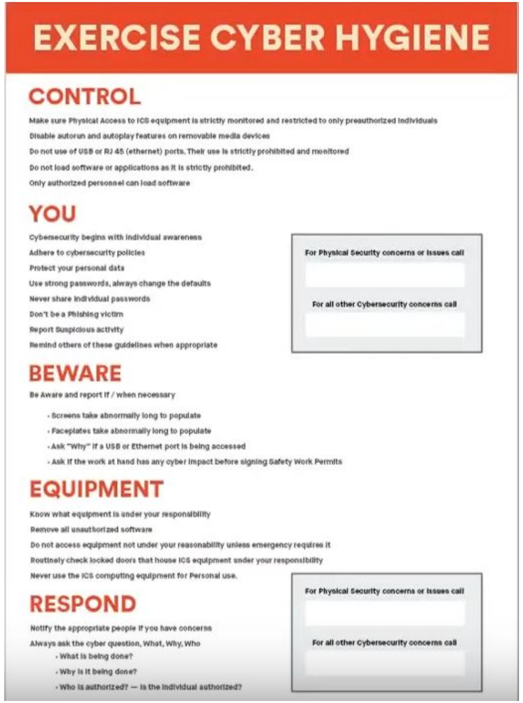
- Use strong passwords
- Close any unused accounts
- Maintain updated devices
- Adheer to company policies (25% of employees admit to ignoring company security policies.
- Limit personal information on social media
- Report suspicious network activity

DON'T

- Reuse passwords for multiple accounts
- Share accounts with multiple people
- Use personal devices for business activities
  (56% of employees use personal computer for work from home)

Employees should be clearly informed for their responsibility for cybersecurity

- Formally define cyber hygiene requirement in terms of use.
- Clearly communicate expectations for all employees.
- Use flyer and bulletins to provide reminders.



EXERCISE CYBER HYGIENE

CONTROL

Make sure Physical Access to ICS equipment is strictly monitored and restricted to only preauthorized individuals

Disable autorun and autoplay features on removable media devices

Do not use of USB or RJ 45 (ethernet) ports. Their use is strictly prohibited and monitored

Do not load software or applications as it is strictly prohibited.

Only authorized personnel can load software

YOU

Cybersecurity begins with individual awareness

Adhere to cybersecurity policies

Protect your personal data

Use strong passwords, always change the defaults

Never share individual passwords

Don't be a Phishing victim

Report Suspicious activity

Remind others of these guidelines when appropriate

For Physical Security concerns or issues call

For all other Cybersecurity concerns call

BEWARE

Be Aware and report if / when necessary

- Screens take abnormally long to populate
- Faceplates take abnormally long to populate
- Ask "Why" if a USB or Ethernet port is being accessed
- Ask if the work at hand has any cyber impact before signing Safety Work Permits

EQUIPMENT

Know what equipment is under your responsibility

Remove all unauthorized software

Do not access equipment not under your reasonability unless emergency requires it

Routinely check locked doors that house ICS equipment under your responsibility

Never use the ICS computing equipment for Personal use.

RESPOND

Notify the appropriate people if you have concerns

Always ask the cyber question, What, Why, Who

- What is being done?
- Why is it being done?
- Who is authorized? — is the individual authorized?

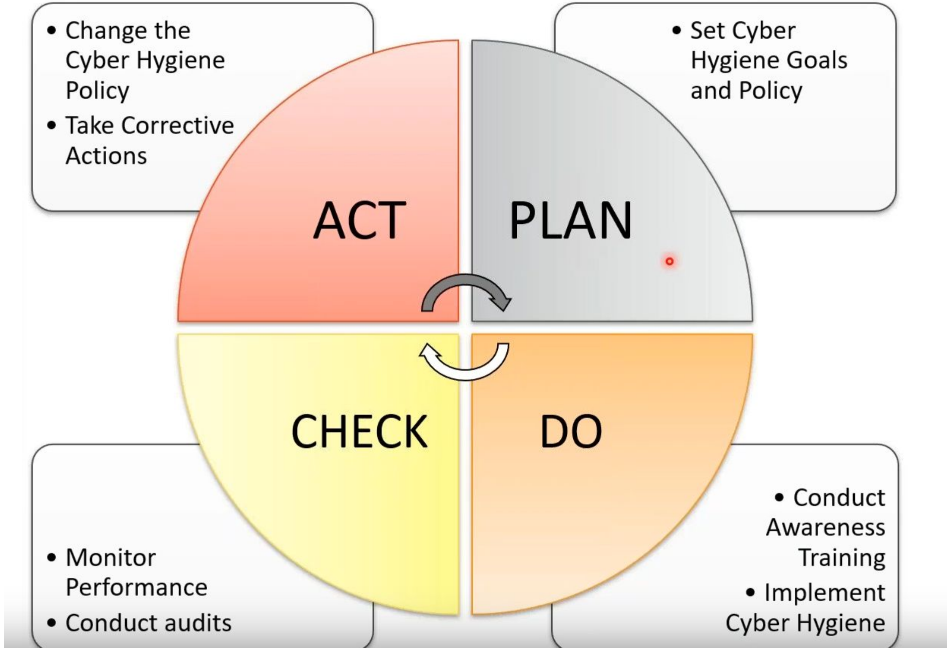
For Physical Security concerns or issues call

For all other Cybersecurity concerns call

Enroll employees in periodic awareness training

- Ensure all employees are given automation specific awareness training.
- Use questions to gauge understanding
- Revalidate training on a yearly basis
- Use Learning Management Systems (LMS) to share training and track compliance

Adopt a continuous improvements approach



- Change the Cyber Hygiene Policy
- Take Corrective Actions

ACT

PLAN

- Set Cyber Hygiene Goals and Policy

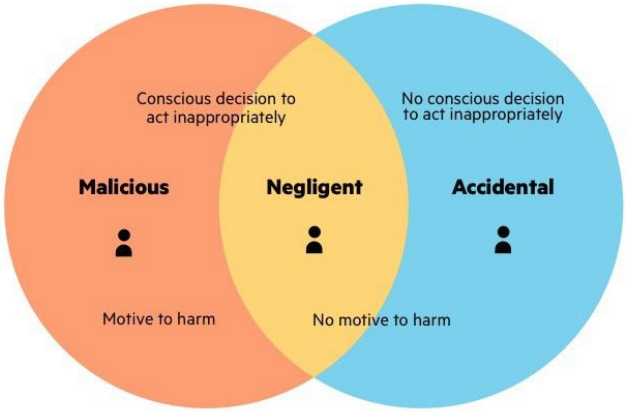
CHECK

DO

- Monitor Performance
- Conduct audits

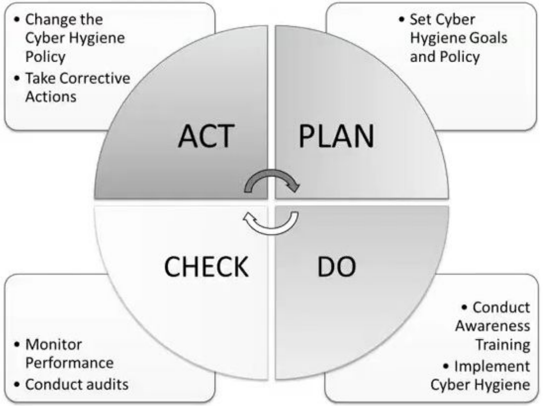
- Conduct Awareness Training
- Implement Cyber Hygiene

This presentation covered the importance of cyber hygiene cyber hygiene basics and implementation strategies


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

Why is cybersecurity Hygiene important for automation systems?

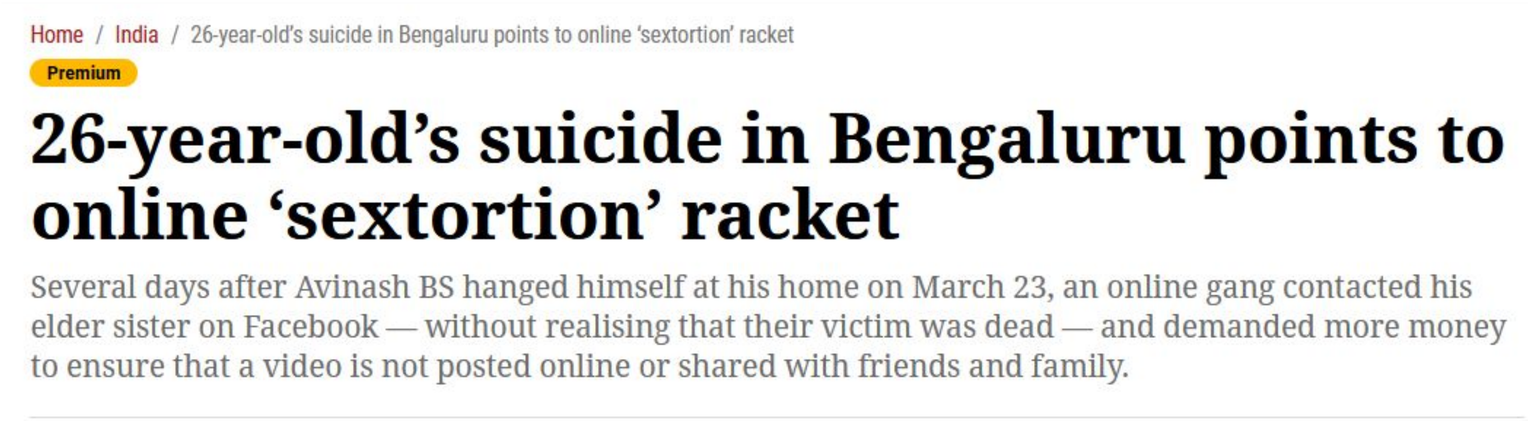
Why is cybersecurity hygiene important for automation systems?



How to Implement Cybersecurity Hygiene?

Case study time!

Case Study- 1



Home / India / 26-year-old’s suicide in Bengaluru points to online ‘sextortion’ racket

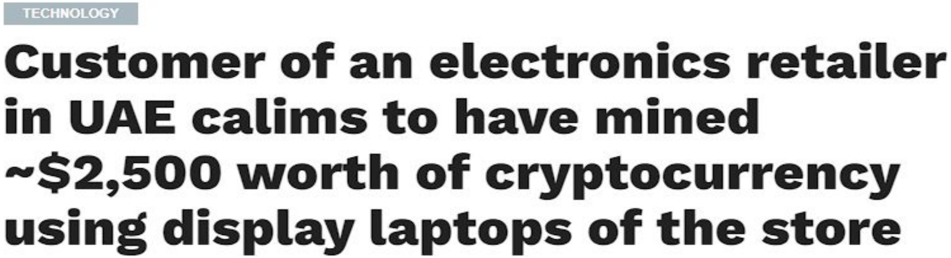
Premium

26-year-old’s suicide in Bengaluru points to online ‘sextortion’ racket

Several days after Avinash BS hanged himself at his home on March 23, an online gang contacted his elder sister on Facebook — without realising that their victim was dead — and demanded more money to ensure that a video is not posted online or shared with friends and family.

Reference:- https://www.newcmi.com/blog/tips-for-detecting-a-phishing-email

Case Study- 2



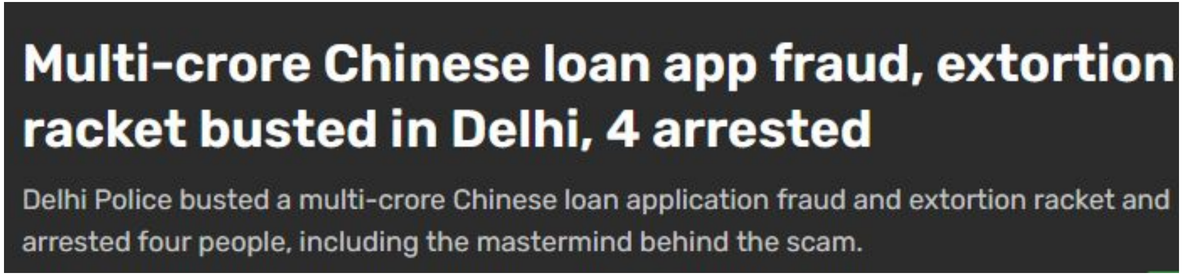
TECHNOLOGY

Customer of an electronics retailer in UAE calims to have mined ~$2,500 worth of cryptocurrency using display laptops of the store

Sharaf DG .com

Reference:-
http://www.menabytes.com/sharaf-dg-mining-xmr/

Case Study- 3

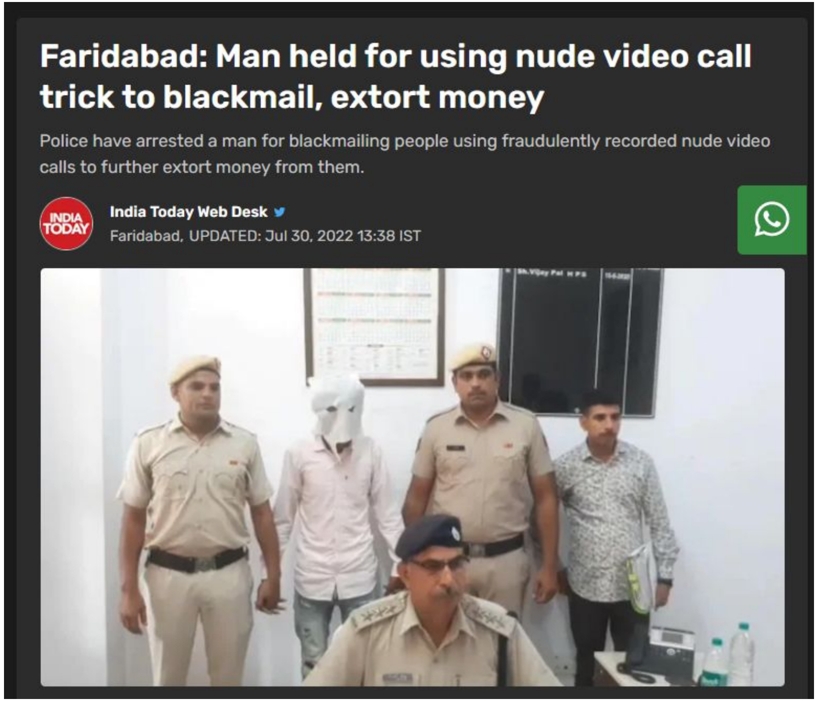


Multi-crore Chinese loan app fraud, extortion racket busted in Delhi, 4 arrested

Delhi Police busted a multi-crore Chinese loan application fraud and extortion racket and arrested four people, including the mastermind behind the scam.

CYBER POLICE STATION
OUTER NORTH DISTRICT
साइबर
CYBER P
OUTER NORTH DI

Case Study- 4

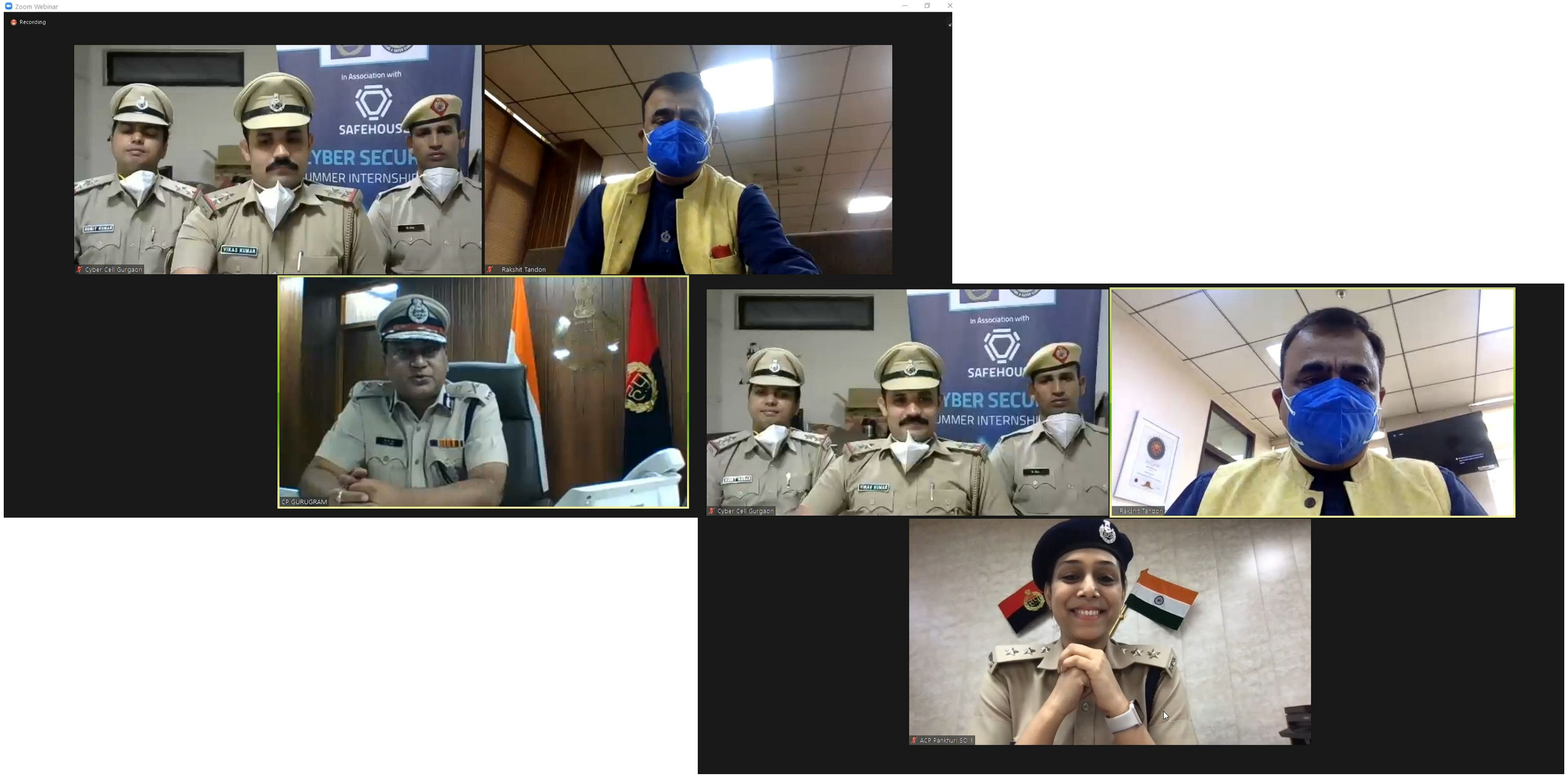


Faridabad: Man held for using nude video call trick to blackmail, extort money

Police have arrested a man for blackmailing people using fraudulently recorded nude video calls to further extort money from them.

India Today Web Desk

Faridabad, UPDATED: Jul 30, 2022 13:38 IST


Zoom Webinar
Recording
In Association with
SAFEHOUSE
YBER SECUR
UMMER INTERNSHI
SUMIT KUMAR
VIKAS KUMAR
Cyber Cell Gurgaon
Rakshit Tandon
CP GURUGRAM
Cyber Cell Gurgaon
Rakshit Tandon
ACP Pankhuri SO 1

Thank You Thank You
Thank You

THANKS!

NIHAR ZUTSHI
nihar.49-cse-19@mietjammu.in
+91 849 38279 13
linkedin.com/niharzutshi