Case Studies on Recent Cyber Attacks

Presentation by:

Cyber Security Centre of Excellence (CS-CoE)

Department of Information Technology & Electronics, Government of West Bengal

Landmark Cyber Attacks / Breaches

AUG 2019

Bihar education department website hacked

- ❑The official website of the Bihar Education Department was hacked on Sunday, with hackers uploading messages in praise of Pakistan on the webpage.
- ❑"RootAyyildiz Turkish Hacker' claimed responsibility for hacking the website and posted messages in praise of Pakistan and Islam.
- ❑Soon after, the website was not accessible and displayed- Service Unavailable. HTTP Error 503 message.

OCT 2019

Kudankulum cyber attack

- ❑The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network
- ❑v
- ❑Identification of malware in NPCIL system
- ❑Dtrack malware - A Spyware in ATM Machines and Company Servers Can Steal Your Money and Data

MAY 2018

Data theft at zomato

- ❑The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities and put up for sale on the Dark Web

FEB 2019

24 websites of central ministries, departments and state governments were hacked

- ❑"As per the information reported **to** and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 199, 172, 110 and 25 **websites of Central Ministries/Departments and State Governments were hacked** during the year 2016, 2017, 2018 and 2019 (**till May**)

Hackers steal Rs. 1.5 Lakh from card without OTP, PIN

Bank says they are investing the case………

Nothing has happened even after 20 days.

All the hacker needs is card number and CVV. Skimming is a method used by identity thieves to capture information from a cardholder.

- Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.
- Some machines act like point-of-sale technology. An acquired card is swiped, and a touch pad allows the user to enter a security code.
- Card users are warned to keep their cards in their sight at all times and to cover the pin pad when inputting security codes

Source: MoneyLife

Turkish cybercriminals hack Tripura ATMs, steal huge cash

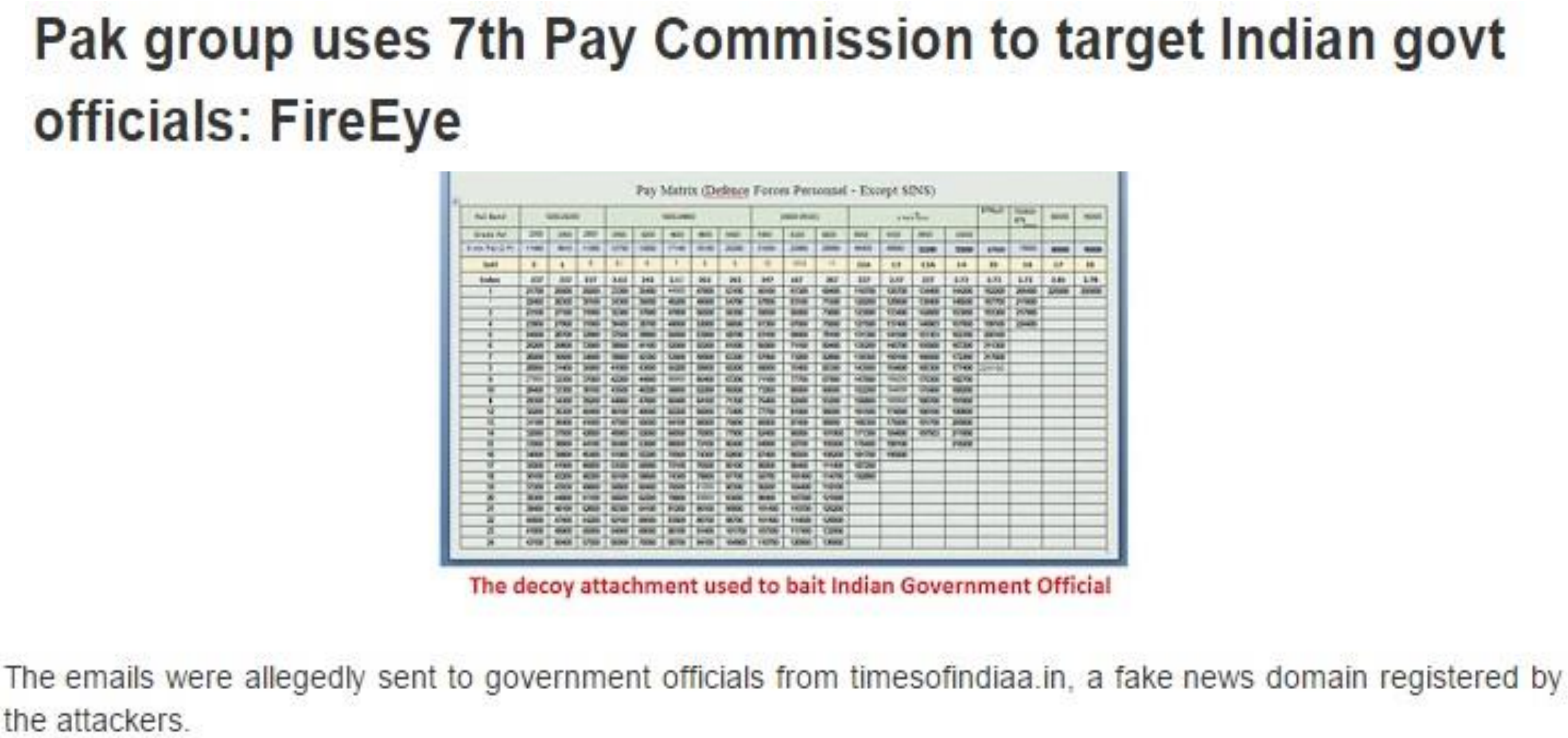
According to the police, banks and other sources, over 60 bank customers of different banks mostly State Bank of India (SBI) during the past few days lost lakhs of rupees due to the fraudulent acts of the cybercriminals and ATM hackers

Over Rs 80 lakhs of several customers were stolen from several ATMs during the past few days in Agartala

According to a cyber-technology expert, the ATM card cloning system comprises a spy camera, a memory card and a small data device to gather ATM and account details of bank customers.

Source: MoneyLife

Seventh Pay Commission: Know how Pak based cyber attackers lured Indian govt. officials



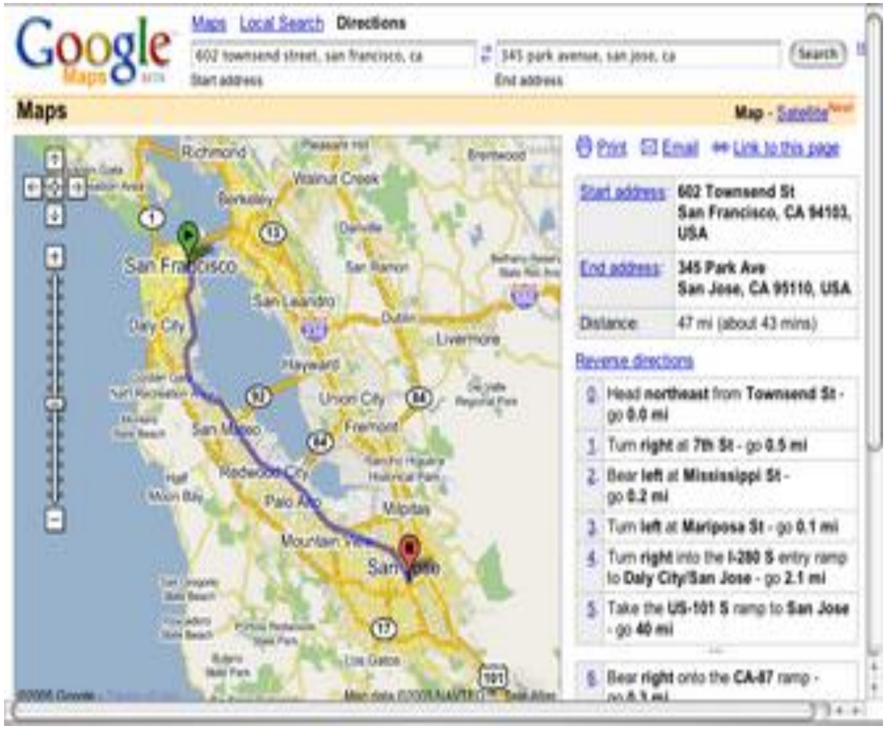
Pak group uses 7th Pay Commission to target Indian govt officials: FireEye

Pay Matrix (Defence Forces Personnel - Except SINS)

The decoy attachment used to bait Indian Government Official

The emails were allegedly sent to government officials from timesofindiaa.in, a fake news domain registered by the attackers.

What happens if you post your photograph on Facebook? Data Privacy issues… Do You have a Social Media Policy?



Start address: 602 townsend street, san francisco, ca

End address: 345 park avenue, san jose, ca

Start address:	602 Townsend St San Francisco, CA 94103, USA
End address:	345 Park Ave San Jose, CA 95110, USA
Distance:	47 mi (about 43 mins)

0. Head **northeast** from **Townsend St** - go **0.0 mi**
1. Turn **right** at **7th St** - go **0.5 mi**
2. Bear **left** at **Mississippi St** - go **0.2 mi**
3. Turn **left** at **Mariposa St** - go **0.1 mi**
4. Turn **right** into the **I-280 S** entry ramp to **Daly City/San Jose** - go **2.1 mi**
5. Take the **US-101 S** ramp to **San Jose** - go **40 mi**
6. Bear **right** onto the **CA-87** ramp - go **0.3 mi**

ISI laying honeytraps on Facebook and Twitter to snare Indian defence personnel

Fake Facebook profile, chats through WhatsApp: How suspected ISI agent 'honey-trapped' Army personnel

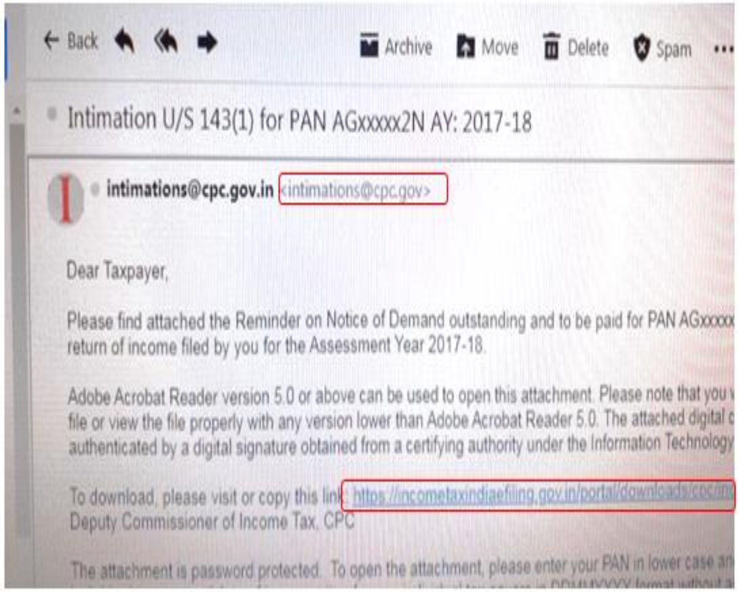
Co – Op Bank Attack -- Events..

xxth August – 20xx – ATM attack

- **2.30 PM received a call** – Large number of Transactions are **Declining**
- **3.30 PM received a call** – Large number of transactions are **Approved & Declining**
- **5.30 PM received a call** – Large number of Transaction are **Approved.**
- **5.47 PM Bank Disconnected Switch with VISA switch** – All Internationals transactions gets stopped.
- **6.00 PM received a call from Indian Customer** – Random Balance Amount, No checking, Accepting Wrong Pin…
- **8.00 PM, disconnected the NPCI Switch**
- **Rs. Xxxx + Crores lost; xxxx + Fraudulent Transactions**.
- Same Card, different Countries, number of Transactions, Velocity Check(?)
- **Bank not aware about the transactions…**

Co-operative Bank's…

1 The attackers used spear-phishing mails for the initial compromise of the systems



Intimation U/S 143(1) for PAN AGxxxxx2N AY: 2017-18

intimations@cpc.gov.in <intimations@cpc.gov>

Dear Taxpayer,

Please find attached the Reminder on Notice of Demand outstanding and to be paid for PAN AGxxxxx
return of income filed by you for the Assessment Year 2017-18.

Adobe Acrobat Reader version 5.0 or above can be used to open this attachment. Please note that you
file or view the file properly with any version lower than Adobe Acrobat Reader 5.0. The attached digital
authenticated by a digital signature obtained from a certifying authority under the Information Technology

To download, please visit or copy this link https://incometaxindiaefiling.gov.in/portal/downloads/cpc/in
Deputy Commissioner of Income Tax, CPC

The attachment is password protected. To open the attachment, please enter your PAN in lower case an

2 Installed Keylogging and Remote Access Tool's on the compromised systems

3 Stolen the authentication credentials & digital certificates

4 Performed fraudulent transactions from external IP addresses using stolen digital certificates

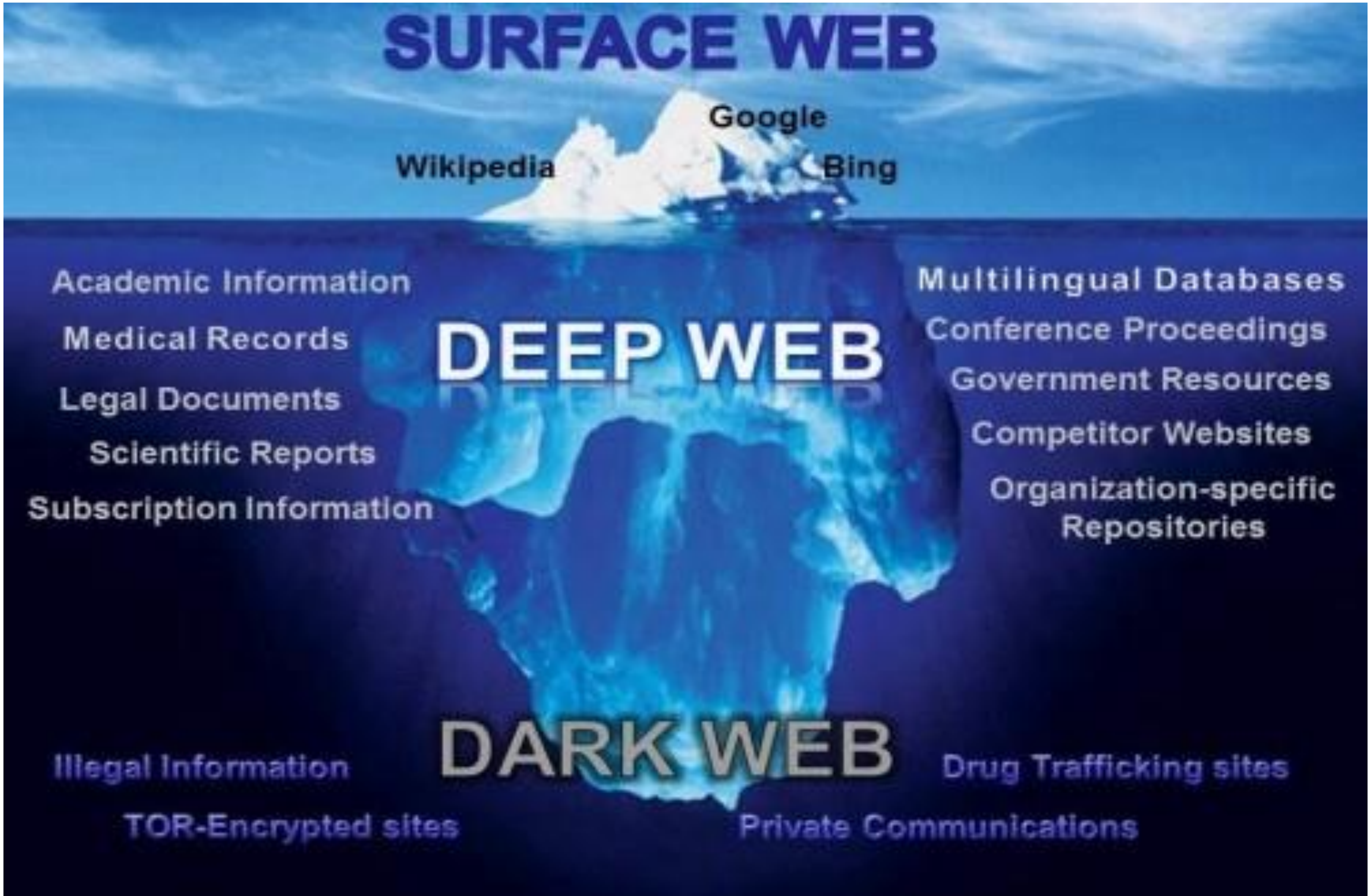
Ransomware - advanced type of malware that restricts access to the computer system until the user pays a fee

Malware - malicious software. Piece of software written with the intent of damaging devices, stealing data. Viruses, Spyware and Ransomware are among the different kinds of malware

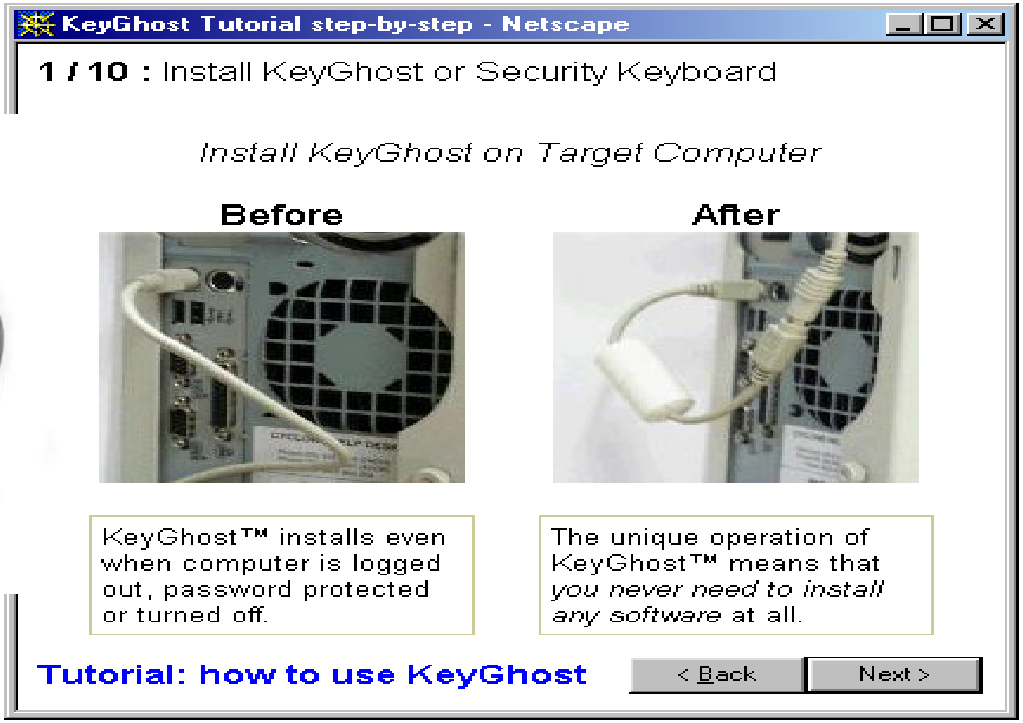
Pegasys - Pegasus is capable of reading text messages, tracking calls, collecting passwords, tracing the location of the phone, accessing the target device's microphone(s) and video camera(s), and gathering information from apps.

Honeytrap - Honey trapping is an investigative practice involving the use of romantic relationships for interpersonal, political or monetary purpose.

***Dark Web* -** part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable



How many of you check… Hardware Key- Logger Do you have a Data Leakage Prevention Policy?



1 / 10 : Install KeyGhost or Security Keyboard

Install KeyGhost on Target Computer

Before

After

KeyGhost™ installs even when computer is logged out, password protected or turned off.

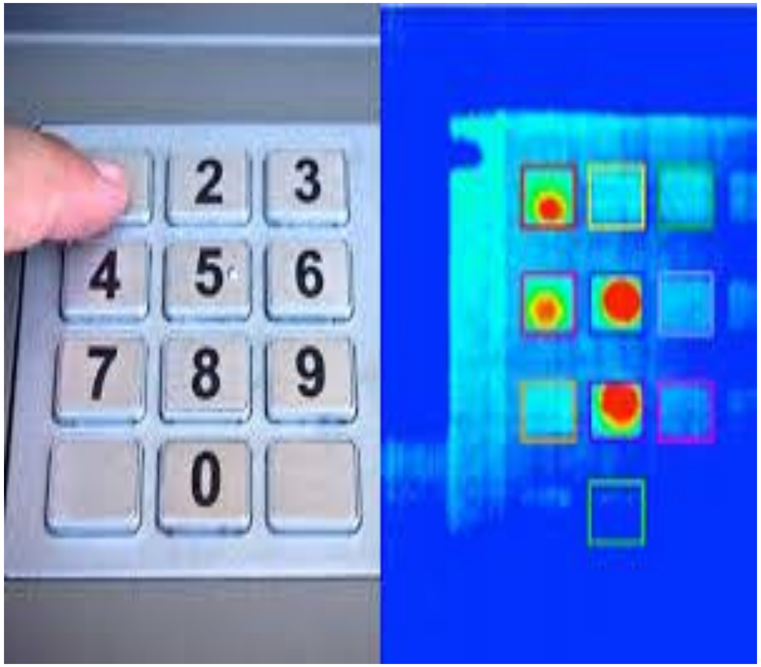
The unique operation of KeyGhost™ means that *you never need to install any software* at all.

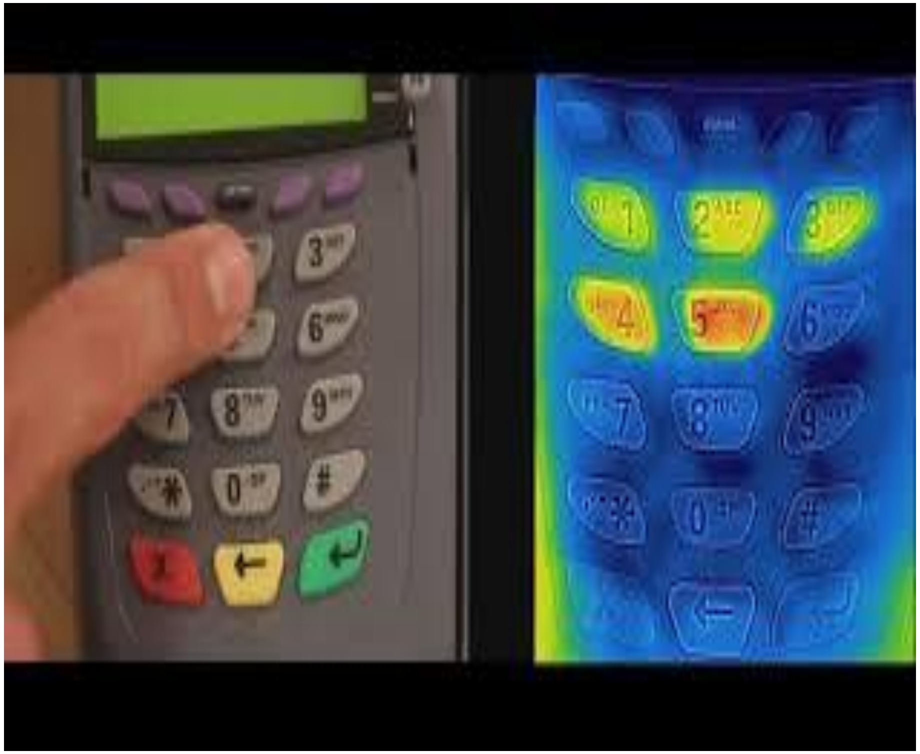
Tutorial: how to use KeyGhost

1. Don’t leave computer unattended with sensitive information on screen
2. Always lock your computer when leaving it unattended with “windows + L” or “ctrl+alt+del”
3. Make sure all vendor updates to the applications/ software you are using is getting updated on a regular basis

2013 Incident

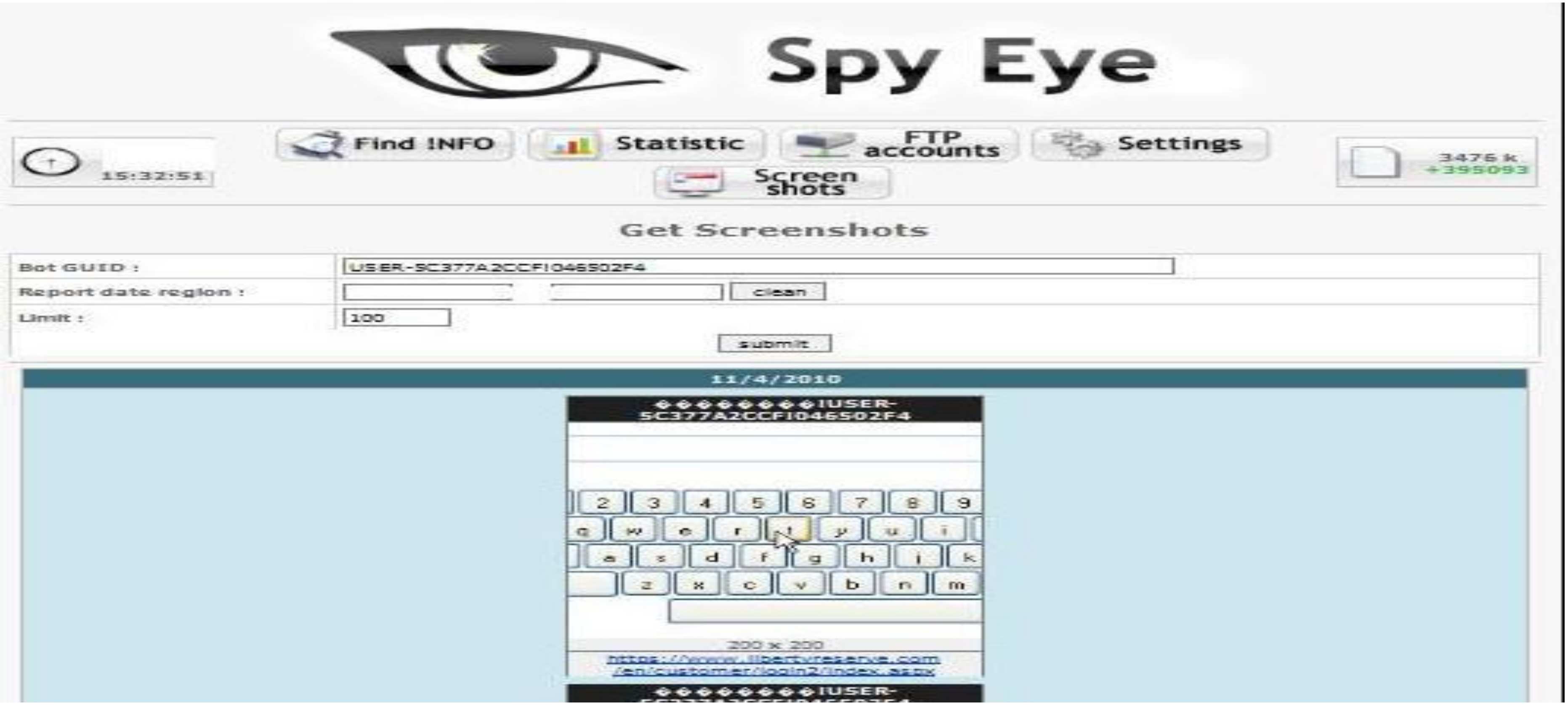
- Which ATM better – First PIN or Last PIN
- Plastic buttons or Metal buttons?





1. Do not share your credit/debit card number, CVV2 code or PIN with anyone
2. When making online payments, make sure that the green padlock and https symbols are active and valid. Do not enter card details in any unverified website/ application or portal
3. When using card in ATM or POS machines, ensure that the device where the card is being used has not been tampered with.

Form Grabbing – Spam Mail filtering….



Get Screenshots

Bot GUID : USER-5C377A2CCF1046502F4

Report date region :

Limit : 100

11/4/2010

◆◆◆◆◆◆◆◆◆IUSER-5C377A2CCF1046502F4

https://www.libertyreserve.com/en/customer/login2/index.aspx

◆◆◆◆◆◆◆◆◆IUSER-

1. Always use genuine vendor software and operating system
2. Always use password protection for your laptop/ mobile device
3. Always use licensed anti-virus software
4. Do not download any software from untrusted sources
5. Do not keep any applications or software which you do not regularly use

Thank you