Identity Theft and Protecting Your Internet Accounts from Hackers

NRC Office of the Inspector General
March 13, 2018

1

Objectives

This presentation will help you prevent cyber hackers from stealing :

- Proprietary information
- Government information
- Contract information
- Internet accessible account Information
- Bank/financial account information

You will also learn about:

- Ransomware
- NRC OIG
- Activities of NRC OIG's Cyber Crimes Unit

2

Inspector General

NRC Inspector General Hubert T. Bell
(Also serves as IG for the Defense Nuclear Facilities Safety Board – DNFSB)

- Appointed by President
  - Advice and consent of the Senate
- Works under "general supervision" of Chairman
- Dual reporting responsibilities
  - Chairman
  - Congress

3

OIG Responsibilities & Authority

Responsibilities:

- Conduct audits and investigations
- Promote integrity and efficiency
- Prevent and detect fraud, waste, and abuse

Authority:

- Access agency records
- Employee cooperation
- Subpoena authority
- Law enforcement authority

Council of the Inspectors General on Integrity and Efficiency

4

OIG Investigations Programs Cyber Crimes Unit (CCU)

- Dedicated OIG Intrusions and Forensic Special Agents and Investigative Analyst
- Investigate intrusions of NRC systems and targeted credential harvesting attempts
- Investigate misconduct involving electronic equipment
- Conduct computer forensic support to agency and OIG
- Offsite forensic Lab
- Member of FBI Cyber Task Force

5

Discussion Topics

- How are Government & Company employees targeted by Hackers?
- How can Hackers steal your money?
- How can Hackers access your e-mails accounts?
- How Hackers can steal your information in your personal "cloud" account?
- How safe is it to check your e-mail on a hotel computer?
- How concerned should you be about ransomware?

6

What do hackers want?

- Proprietary information
- Contract bidding information to win a bid
- design documents
- Your money via online financial accounts
- Ransom money

7

Where do they get it?

- Computers in your organization
- Your personal computers
- Cloud space computers containing your email
- Your email accounts
- Public computers you use
- Thumb drives, especially unencrypted
- Listening to you in public places

8

How do the Cyber Criminals get your info?

- You accidentally give them your password
- You download a file
- You email documents to the Hackers
- Sensitive documents on your personal email
- thumb drive

9

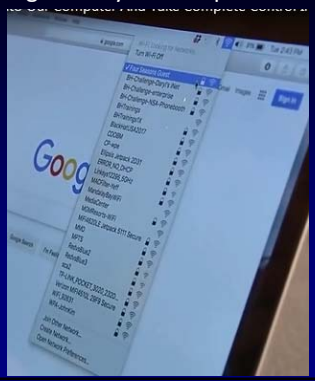
How do the Cyber Criminals get your info?

- Monitoring software
- Hackers find your "password book"
- A remote desktop session with a hacker
- Your home computer is set to Sharing
- "Hi, you won the Lottery $10,000!!! Download this file for instructions." (malicious software)

10

Hotel Wifi

- Can hackers get into your computer through Wi-Fi at Hotels?



11

Phishing Scams

- A Hacker's goal is to get your password

Beware of phishing scams. Don't take the bait! Be suspicious of anyone that asks for your personal information.

12

Phishing Scams

From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Outlook

Dear Email User,

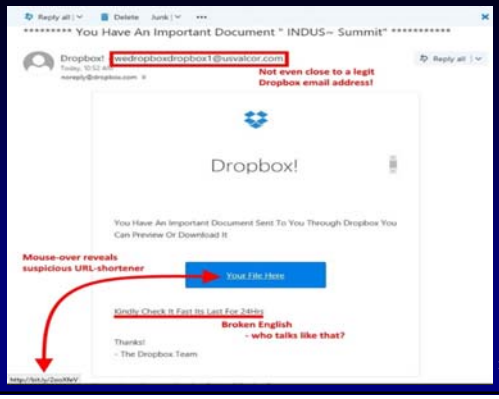
This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security.If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails,and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

Update Your Account

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

13

Phishing Scams



14

Phishing Scams

15

Phishing Scams

From: IRS Online <ahr@irxt.com>
Reply-To: "noreply@irxt.com" <noreply@irxt.com>
Date: Thursday, Apri
Subject: Final reminder: Notice of Tax Return. ID:

IRS

Department of the Treasury
Internal Revenue Service

04.
Reference:

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

16

Ransomware

- Malicious software
- Downloading/executing a malicious payload
- JavaScript based now
- Buried inside email attachments
- Via poisoned websites
- Through exploit kits
- On infected USB devices and network worms
- Email attachments containing fake invoices
- Ransomware payments are demanded via Bitcoin

17

Ransomware

- Bitcoin is a new currency accessible via internet
  - no middle men – meaning, no banks
  - Anonymous transfer of money
  - Untraceable!

18

Ransomware

In May 2017, WannaCry. Approximately 230,000 computers in 150 countries affected.

In June 2015, nearly 1,000 victims called the FBI for help regarding **CryptoWall** infections. Estimated losses of at least $18 million.

In November 2014, over 9,000 infected by TorrentLocker in Australia. In Turkey 11,700 infected.

19

Hotel Computers

- Encrypted thumb drives
- Email

20

Internet Café, Public Places

- Email
- Bank account
- PayPal

21

Friend's computer

- hacked previously
- remote software
- thumb drive

22

"Internet Cafe"

- Public computer, hotel, school
- Internet Cache
- Downloads folder
- Recycle bin
- Serial # of your thumb drive
- Email and TIF images
- Metadata

23

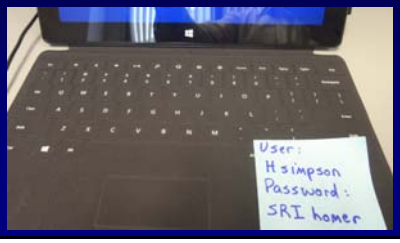
Cloud

- Gmail, Yahoo email, Hotmail, …Where is my email stored?
- Large companies sell data space in their cloud warehouses.
- Warehouse with many computer HDs or SSDs, accessible via internet login
- MS Outlook

24

Do you write your password where someone can see it?

- Post it Notes
- Cleaning crew
- Visitors
- Teenage children view porn at night
- Security violation or computer misuse?



25

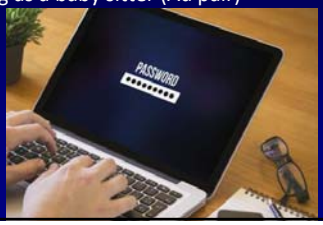
Do you use the same password for all your accounts?

- Same password for all internet accounts?
- Online bank account and tennis club membership?
- Email account same as tennis club?
- Secretary, wife, or children?
  - Do they protect your password as well as you do?

26

Does your home/business computer have a Password?

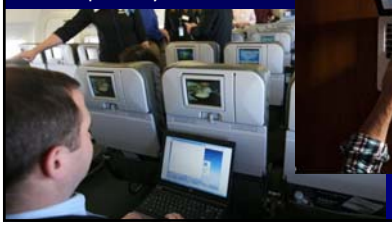
- Anyone can open it and access everything
- Children's friends
- Baby sitter
- Cleaning company
- Spy working for a cleaning company
- Spy posing as a baby sitter (Au pair)



27

Anyone looking over your shoulder?

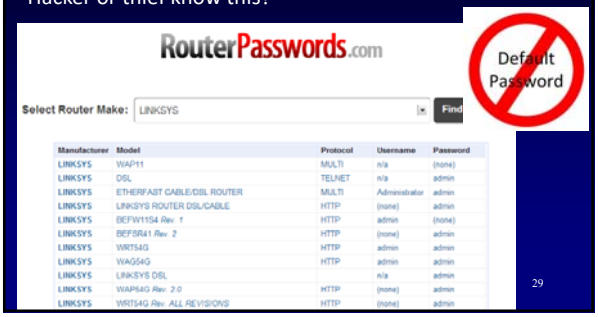
- When you log into your email, Bank account, PayPal?
  - Airplane - space between seats
  - Coffee Shop
  - Hotel Lobby
  - Classified data?
  - Company formula?
  - Proprietary info?



28

Password "admin" default on Router

- How long is your password?
- Still set to the standard default password?
- Default password same for all devices similar to yours?
- Hacker or thief know this?



29

Separate username accounts for shared computers?

- Wife downloaded CP on husbands computer
- User account for each, with password
- All activity and documents stored separately from yours

30

Hackers might steal your mail or dig through your trash

- Pin # to your ATM card and CC for cash withdrawal
- Pin # to file your income tax return
- Credit Card checks for cash withdrawal
- New Checking account checks from your bank
- Have mail delivered to company while on travel?
- Social Security Number
- Date of Birth
- Traveling for several days?

31

Encrypted thumb drives and external hard drives

- If stolen or lost, all data is secure
  - Proprietary info, classified documents, schoolwork, bank

32

Laws

O.R.S. 164.377 (see also 18 USC 1030 for the Federal computer crime statute):

(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

(a) Devising or executing any scheme or artifice to defraud;

(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

(c) Committing theft, including, but not limited to, theft of proprietary information. [* * *]

(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(5)(a) A violation of the provisions of subsection (2) or (3) of this section shall be a Class C felony. Except as provided in paragraph (b) of this subsection, a violation of the provisions of subsection (4) of this section shall be a Class A misdemeanor.

CCU Investigations of Identity Theft & Against Hackers

A Government employee on travel to a regional office for the first time dined at a known chain restaurant and used his Government travel card to pay for the meal. Two weeks later, there were four separate fraudulent charges totaling $3,000.

OIG found that the employee's waiter skimmed the credit card and sold the account information to an organized group for $50. OIG coordinated with local police, who arrested the waiter.

WHY WAS THE EMPLOYEE TARGETED?

7

CCU Investigations

- Someone using the compromised emails of employees of a state public utilities commission sent an email with subject line, "Account Validation," targeting 20 Government employees. The employees were informed that the "Helpdesk Server" was undergoing mailbox validation and directed to click on a link in the email that took them to a credential harvesting site where they were prompted to enter their network username and password.
- The sender tried again with another email.

35

CCU Investigations

A former Government employee attempted to sell 5,000 Government email addresses for $23,000 to someone he believed was a foreign government official. He also discussed having 30,000 additional Government email accounts. He sought to have the foreign entity use the emails to launch a spear phishing attack against the U.S. Government so that foreign nations would gain access to sensitive information or damage essential systems. In April 2016, the former NRC employee was sentenced to 18 months in prison. The investigation was a joint effort by the FBI, DOE, and NRC OIG.

36

CCU Investigations

Someone was impersonating a Government employee and requesting quotes from different companies for multiple IT equipment. These quotes were for over $115,000. The SUSPECT had created a bogus e-mail account of an actual Government employee, but instead of .gov, an .org account was used. Once the quotes were received the SUSPECT sent fake purchase orders to the companies with a shipping address to a storage unit and A POC at the storage company.

37

CCU Investigations

Someone created a fake Facebook page and was supposedly offering to help people apply for NRC Grants in the amount of $250,000. This person was reaching out to people on his "Friends List" and would offer to help get them the grant for as little as $500. The SUSPECT had taken a real photo and altered it to make it seem he had helped in awarding the check to people.

The real photo is on the left while the altered photo is on the right.

Contact the OIG

Contact:	OIG Hotline 1-800-233-3497 8:00 a.m. to 4:00 p.m. Monday – Friday After hours, please leave a message
Submit:	On-line form, access by logging onto: www.nrc.gov Click on Inspector General Click on OIG Hotline Phone Symbol
Call:	OIG Cyber Crimes Unit Cyber Special Agent Patrick Hanks – 301-415-5925 Patrick.hanks@nrc.gov Cell 301-684-0211 Supervisory Special Agent Malion Bartley – 301-415-5962 Cyber Special Agent Kris Marchant – 301-415-5925

39

Questions?

40