Computer Systems

Lecture : Information Security

Introduction to Information Security

Security Threats

Potential threats to computer security:

- Internal threats
  - Employees can cause a malicious threat or an accidental threat.
- External threats
  - Outside users can attack in an unstructured or structured way.

Types of attacks to computer security:

- Physical
  - Theft, damage, or destruction to computer equipment.
- Data
  - Removal, corruption, denial of access, unauthorised access, or theft of information.

Malware

- **Malware** is malicious software that is installed on a computer without the knowledge or permission of the user.
- Viruses, Worms, Trojans are all part of a class of software called malware.
- Malware is a broad term used to describe all sorts of unwanted or malicious code.
- It may take several different anti-malware programs and multiple scans to completely remove all malicious software.
- Anti-malware available for these purpose are: Anti-virus, anti-spyware, anti-adware, and phishing programs.

Virus

- A software code that is deliberately created by an attacker that propagates by inserting a copy of itself into and becoming part of another program.
- The virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.
- It spreads from one computer to another, leaving infections as it travels.
- It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action, people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments.

Worm

- A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself.
  - One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues …….
- Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding.

Trojan

- A Trojan is malicious software that is disguised as a legitimate program. It is named for its method of getting past computer defences by pretending to be something useful.
- Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system.
- Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

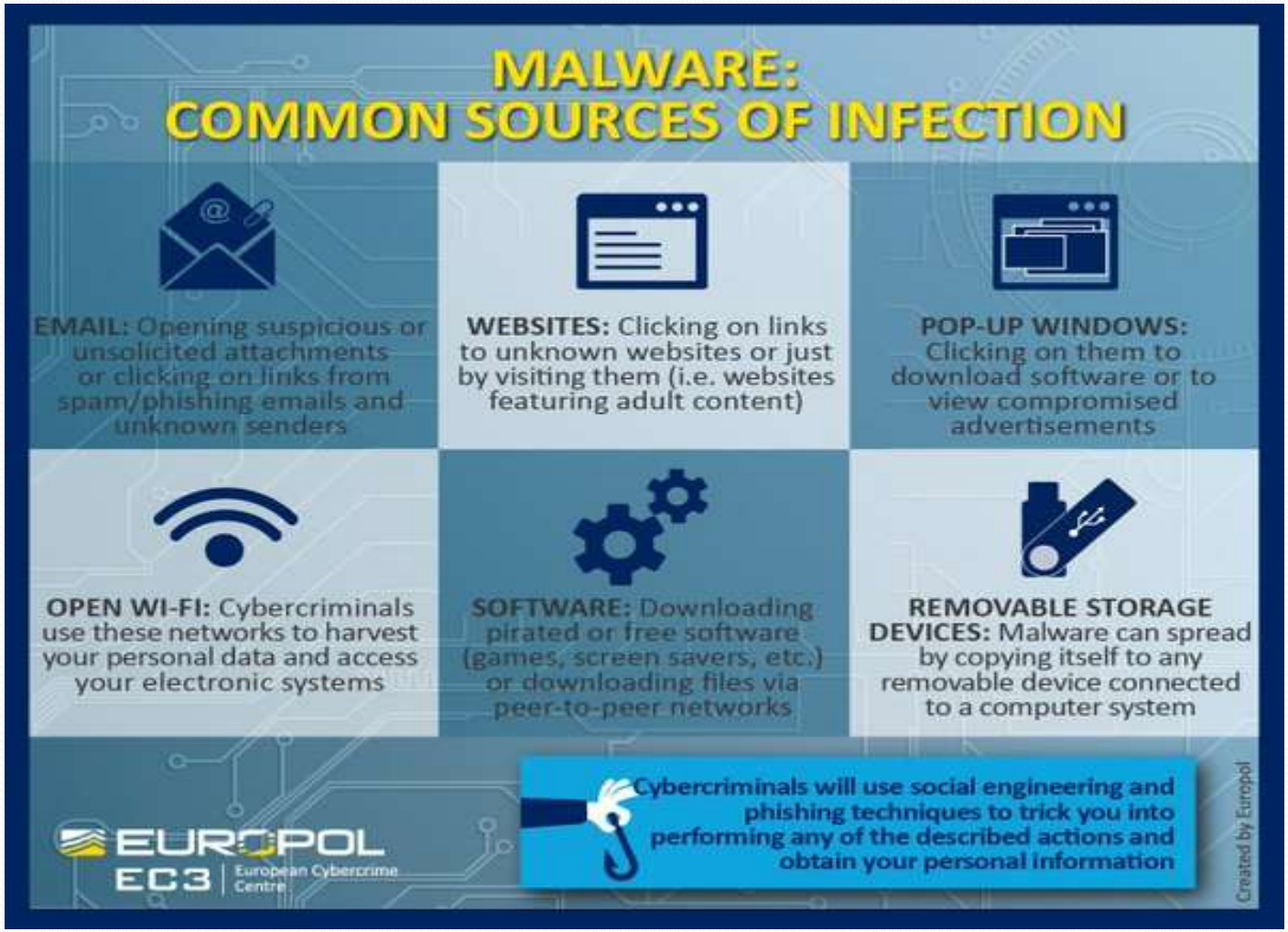
Logic bomb

- It is a piece of computer code that executes a malicious task, such as clearing a hard drive or deleting specific files, when it is triggered by a specific event.
- It's secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs.
- The event could be a date or when a program is opened.
- And when the bomb goes off, the damage is done -- files are deleted, secret information is sent to the wrong people, the network is crippled for days ...

Adware, Spyware & Spam

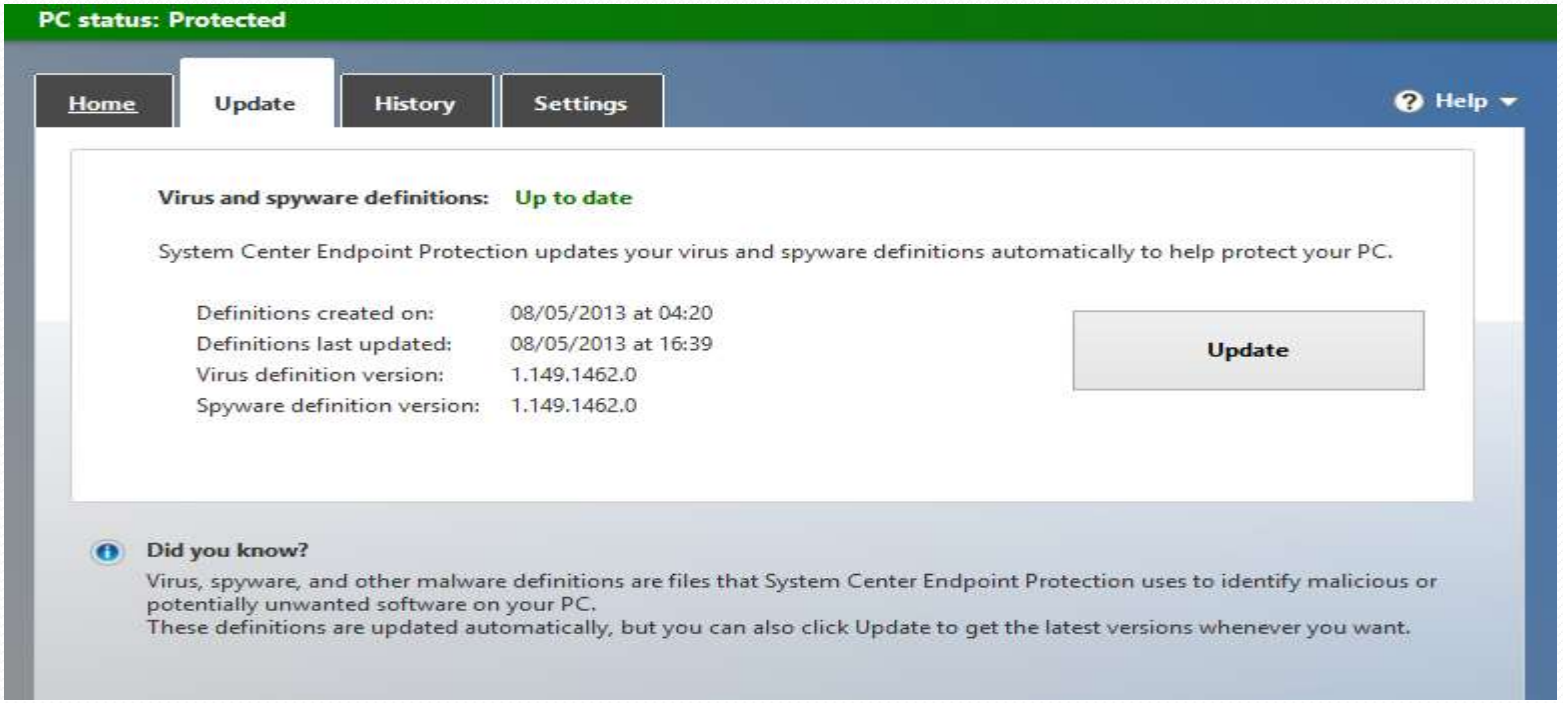
- **Adware** - software program that displays advertising on your computer, often displayed in a pop-up window.
- **Spyware** - distributed without user intervention or knowledge, monitors activity on the computer.
- **Spam** is unsolicited email that can be used to send harmful links or deceptive content.

Malware Infections



AntiVirus

- New viruses are always being developed, therefore security software must be continually updated.



- What about AntiMalware???

Increase In Attacks/Infections

- Cyber attacks have increased dramatically.
- Easy money. Big business means big money.
- Millions and millions of potential victims.
- LACK OF AWARENESS.

Increase In Attacks/Infections

- Everybody has some form of computer.
- Everybody accesses online services.
- Everybody has some form of data on a computer and in the cloud.

- the economy depends on a stable, safe, and resilient online environment
- a vast array of networks allows us to:-

Communicate and **travel**

Power our homes

Run our economy

Provide government services

Internet of Things (IoT)

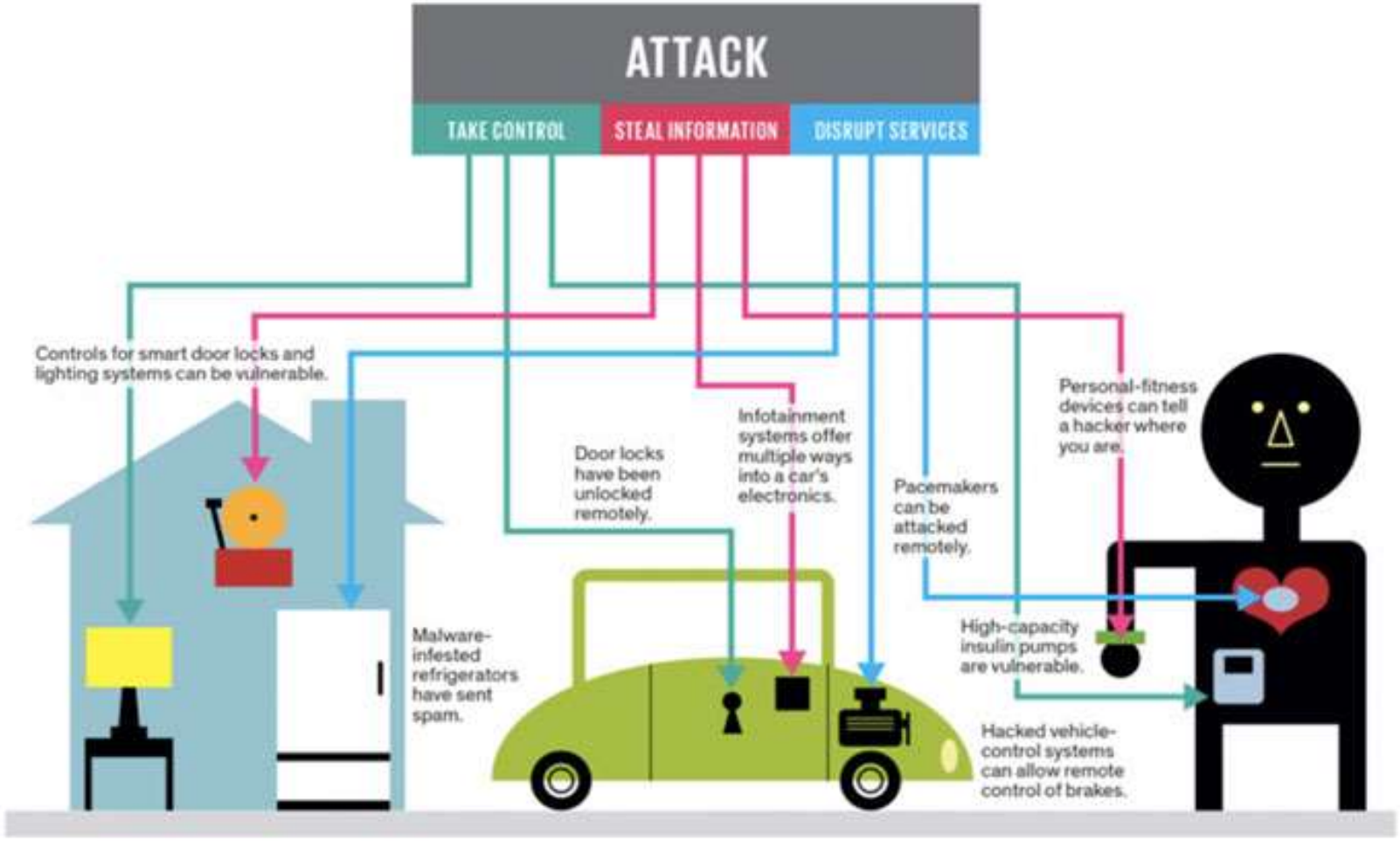


Illustration: J. D. King

Internet of Things (IoT)

BBC Sign in News Sport Weather Shop Earth Travel Mor

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

'Smart' home devices used as weapons in website attack

22 October 2016 | Technology Share

Net-connected cameras are helping attac

BBC Sign in News Sport Weather Shop Earth Travel More

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

Smart LED light bulbs leak wi-fi passwords

By Jane Wakefield
Technology reporter

PCWorld FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Privacy Encryption Antivirus

Home / Security

NEWS

Armies of hacked smart devices launch unprecedented DDoS attacks

DDoS attacks got a power boost thanks to hundreds of thousands of insecure IoT devices

CNBC

HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

ON THE MONEY

ON THE MONEY | VIDEO | WHERE TO WATCH

Suddenly hot smart home devices are ripe for hacking, experts warn

Jennifer Schlesinger | Andrea Day

CNBC

Internet of Things (IoT)

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Parker Higgins @xor · 8 Feb 2015
Left: Samsung SmartTV privacy policy, warning users not to discuss personal info in front of their TV
Right: 1984

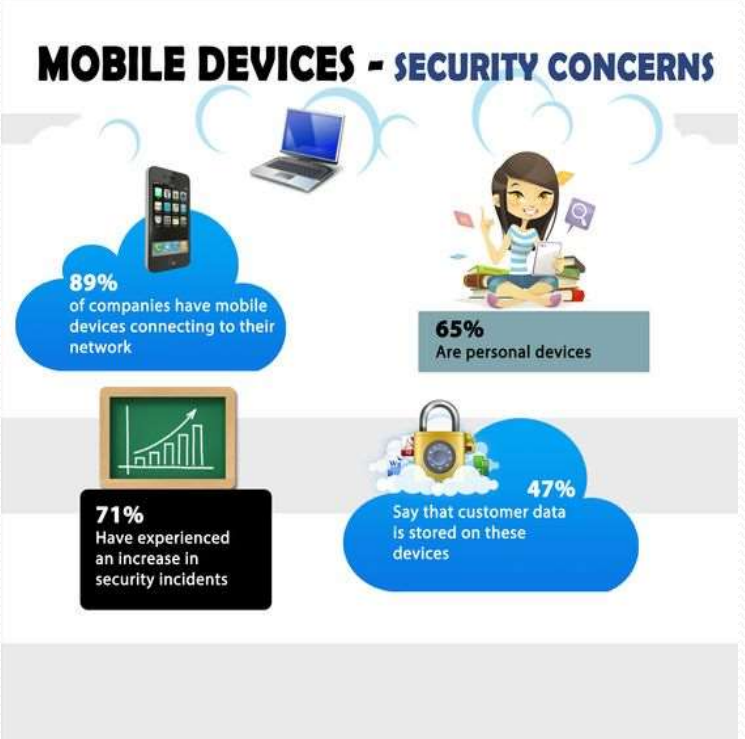
32K 17K

BYOD (Bring Your Own Device)

- BYOD (bring your own device) is the increasing trend toward employee-owned devices within a business, school, coffee shop. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace.

BYOD Concerns

- Insecure Devices
  - Lack of secure Passwords
  - Lack of Encryption
  - Lack of Anti-Virus
- Unauthorised Third Party Access
- Insecure Third Party Apps
- Right to Access (Forensics, eDiscovery)
- Lack of Compliance
- Jailbreaking Devices
- Lack of Patching & Updates
- Insecure Wireless



Insecure/Privacy Apps

- Apps we install require certain features to be enabled.
- These features allow a company or companies access to our data.
- Sometimes this data may be private and not required by the company or we may not wish to supply it.

- What have we allowed?
- Why is it needed?
- Will the app operate without these settings enabled?

QR Codes

- Phishing.
- Malicious software distribution.
- Pointing to potentially harmful websites.

Attacks That Are Big Today

- DDOS (Distributed Denial of Service)
- Phishing
- Ransomware
- Whaling / CEO Fraud
- Social Media Attacks

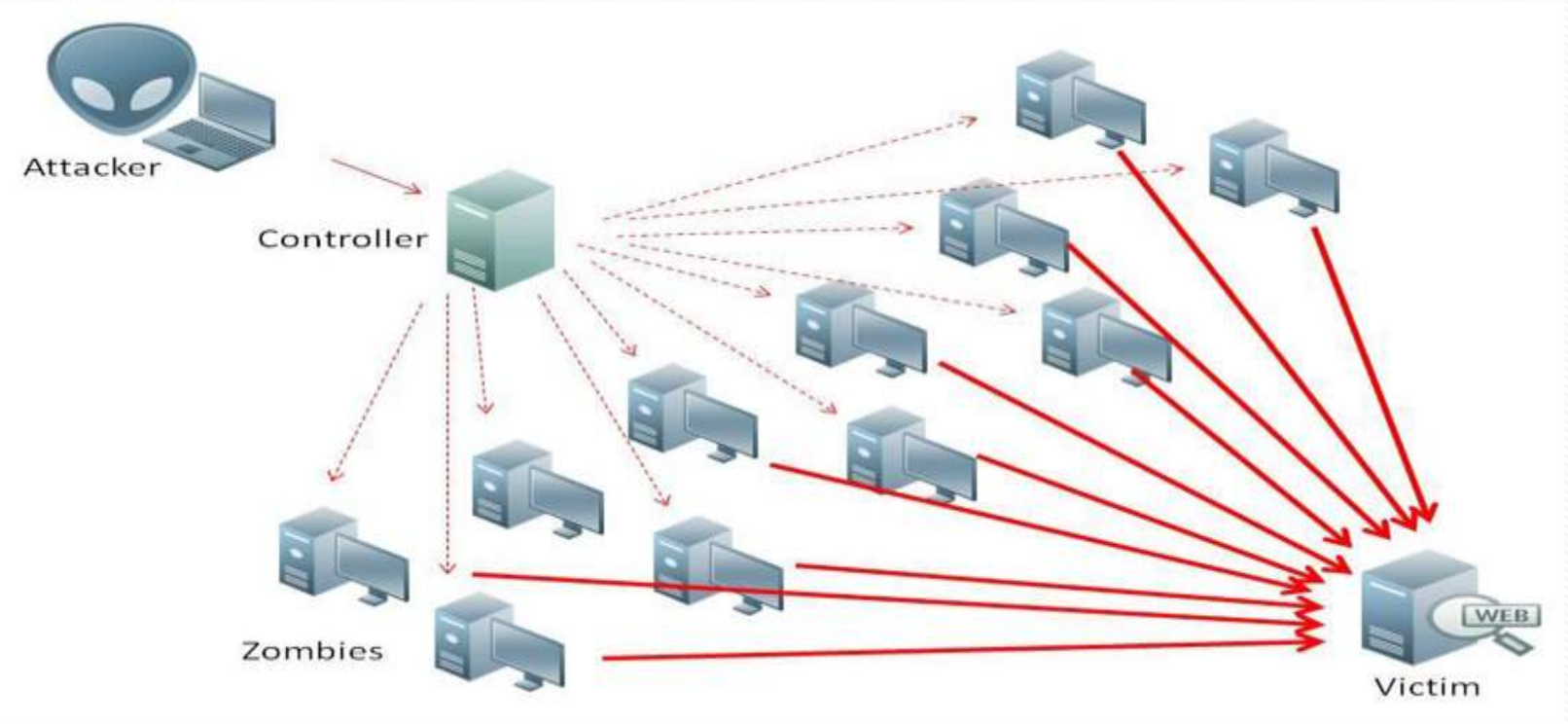
DDOS (Distributed Denial of Service)

- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

- They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

DDOS (Distributed Denial of Service)

- Any unsuspecting device can be used.
- From computers to mobiles, from CCTV to TV's.
- Anything attached to the internet is a potential attacker.



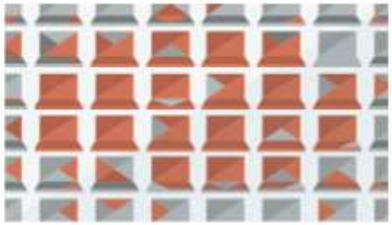
DDOS (Distributed Denial of Service)

- Devices are infected by trojans or installed by hacker on an unprotected device.
- An infected device is called a zombie.
- Once your device is infected, you will never know, it will operate as normal.
- When the time comes to attack a website, all the infected devices, together will send a requests for a specific page (generally the homepage) to the target web site.
- With several requests sent every second from tens of thousands of infected system computers the attack will quickly prove overwhelming to the web site knocking it offline for several days.

DDOS (Distributed Denial of Service)

- One of the biggest attacks used millions of unprotected CCTV's connected to the internet.

Building Capacity



Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Launching Attacks

Botnets can generate huge floods of traffic to overwhelm a target. These floods can be generated in multiple ways, such as sending more connection requests than a server can handle, or having computers send the victim huge amounts of random data to use up the target's bandwidth. Some attacks are so big they can max out a country's international cable capacity.

Selling Silence

Specialized online marketplaces exist to buy and sell botnets or individual DDoS attacks. Using these underground markets, anyone can pay a nominal fee to silence websites they disagree with or disrupt an organization's online operations. A week-long DDoS attack, capable of taking a small organization offline can cost as little as $150.

DDOS (Distributed Denial of Service)

Hello,

To introduce ourselves first:
http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-ex-coin-theft-owner-accuses-ccedk-of-withholding-info
Or just google "DD4BC" and you will find more info.

So, it's your turn! All servers of [REDACTED] group (internationally) are going under DDoS attack unless you pay 40 Bitcoin. Pay to 16HH1Se5zhXgqe4EBAKZxdyMump5Mi-YgrQ Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps. Right now we are running small demonstrative attack on one of your IPs: [REDACTED]. Don't worry, it will not be hard (we will try not to crash it at the moment) and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 40 BTC at the moment, so we are giving you 24 hours to get it and pay us. Find the best exchanger for you on howtobuybit-coins.info or localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet. Current price of 1 BTC is about 250 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 40 BTC to 16HH1Se5zhXgqe4EBAKZx-dyMump5MiYgrQ — we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.

If you need to contact us, use Bitmessage: BM NC1jRewNdHxX3jHrufjxDsRWXGdNisY5 But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 100 BTC and will keep increasing for every hour of attack. Many of our "clients" believe that if they pay us once, we will be back. That's not how we work - we never attack the same target after we are paid. If you are thinking about reporting this to authorities, feel free to try. But it won't help. We are not amateurs.

REMEMBER THIS: It's a one-time payment. Pay and you will not hear from us ever again!
We do bad things, but we keep our word.
Thank you

****

Phishing

- A phishing attempt is a fraudulent attempt, usually made through email, to steal your ‘personal’ information or ultimately deliver some kind of malicious application to your PC.

- Typically a victim receives a message that appears to have been sent by a known contact or organisation.

- An attachment or links in the message may install malware on the user’s device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing Examples

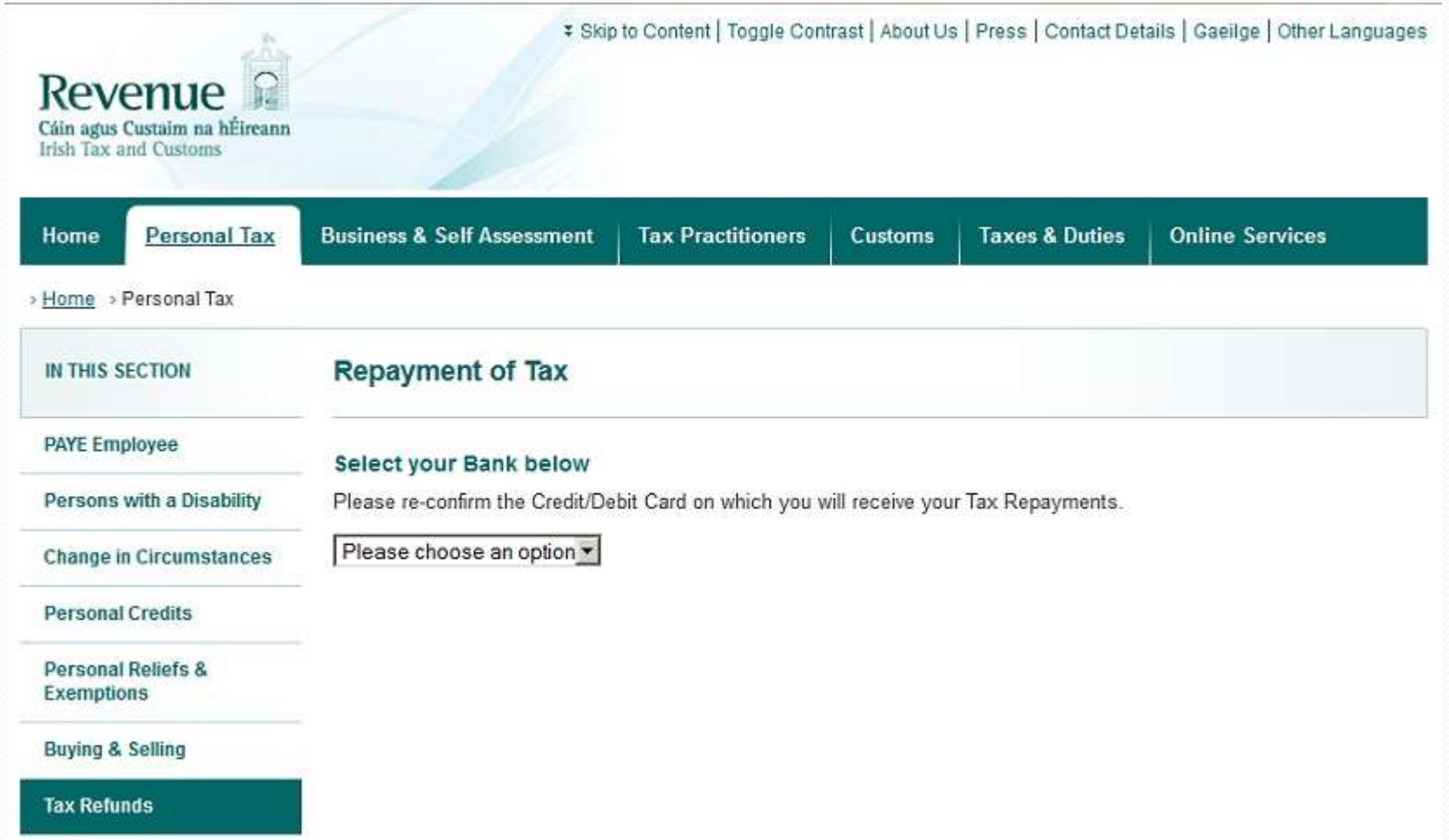
On 08/08/2016 you are scheduled to be charged 9.99 € for your 10 GB iCloud storage plan, but there is a problem with your payment information.
Be sure to update your payment information as soon as possible. Your account will be downgraded to the free 5 GB storage plan if we cannot successfully renew your subscription.

To update your payment information Click here.

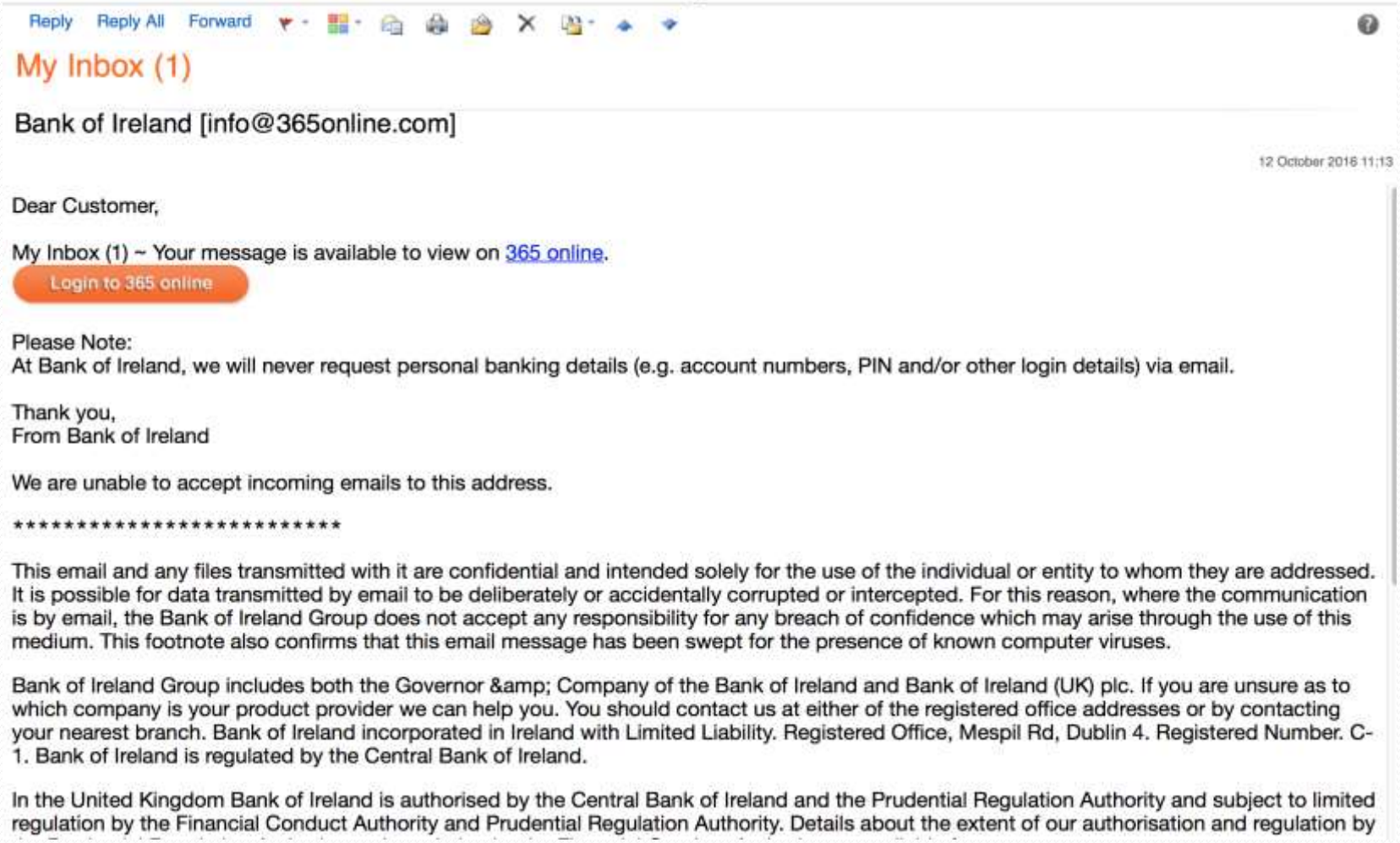
The iCloud Team

iCloud is a service provided by Apple.
Copyright © 2016 Apple Inc.

Phishing Examples



Phishing Examples



Reply Reply All Forward

My Inbox (1)

Bank of Ireland [info@365online.com]

12 October 2016 11:13

Dear Customer,

My Inbox (1) ~ Your message is available to view on 365 online.

Login to 365 online

Please Note:
At Bank of Ireland, we will never request personal banking details (e.g. account numbers, PIN and/or other login details) via email.

Thank you,
From Bank of Ireland

We are unable to accept incoming emails to this address.

****

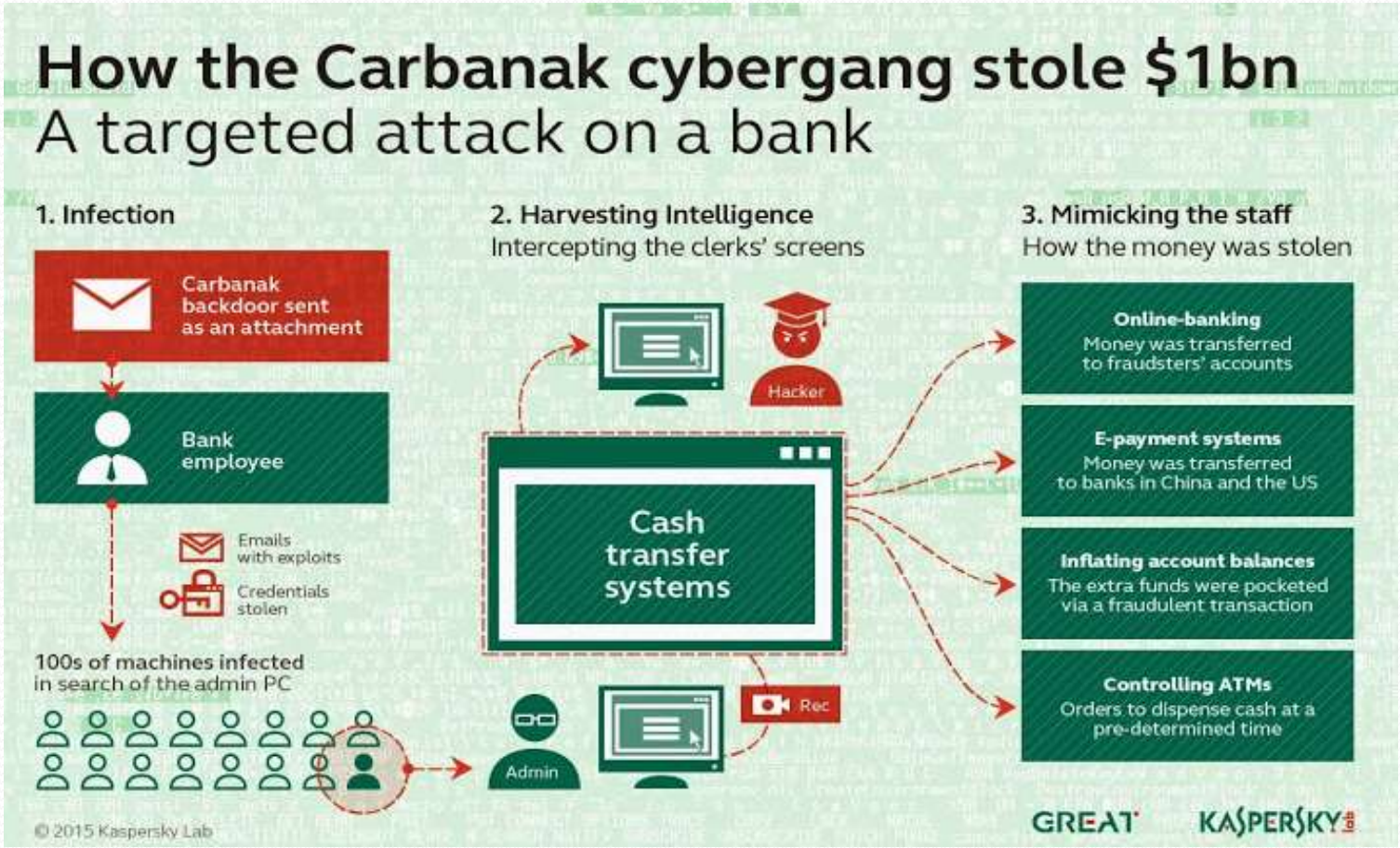
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. It is possible for data transmitted by email to be deliberately or accidentally corrupted or intercepted. For this reason, where the communication is by email, the Bank of Ireland Group does not accept any responsibility for any breach of confidence which may arise through the use of this medium. This footnote also confirms that this email message has been swept for the presence of known computer viruses.

Bank of Ireland Group includes both the Governor & Company of the Bank of Ireland and Bank of Ireland (UK) plc. If you are unsure as to which company is your product provider we can help you. You should contact us at either of the registered office addresses or by contacting your nearest branch. Bank of Ireland incorporated in Ireland with Limited Liability. Registered Office, Mespil Rd, Dublin 4. Registered Number. C-1. Bank of Ireland is regulated by the Central Bank of Ireland.

In the United Kingdom Bank of Ireland is authorised by the Central Bank of Ireland and the Prudential Regulation Authority and subject to limited regulation by the Financial Conduct Authority and Prudential Regulation Authority. Details about the extent of our authorisation and regulation by

Phishing Examples

Successful Phishing Attack

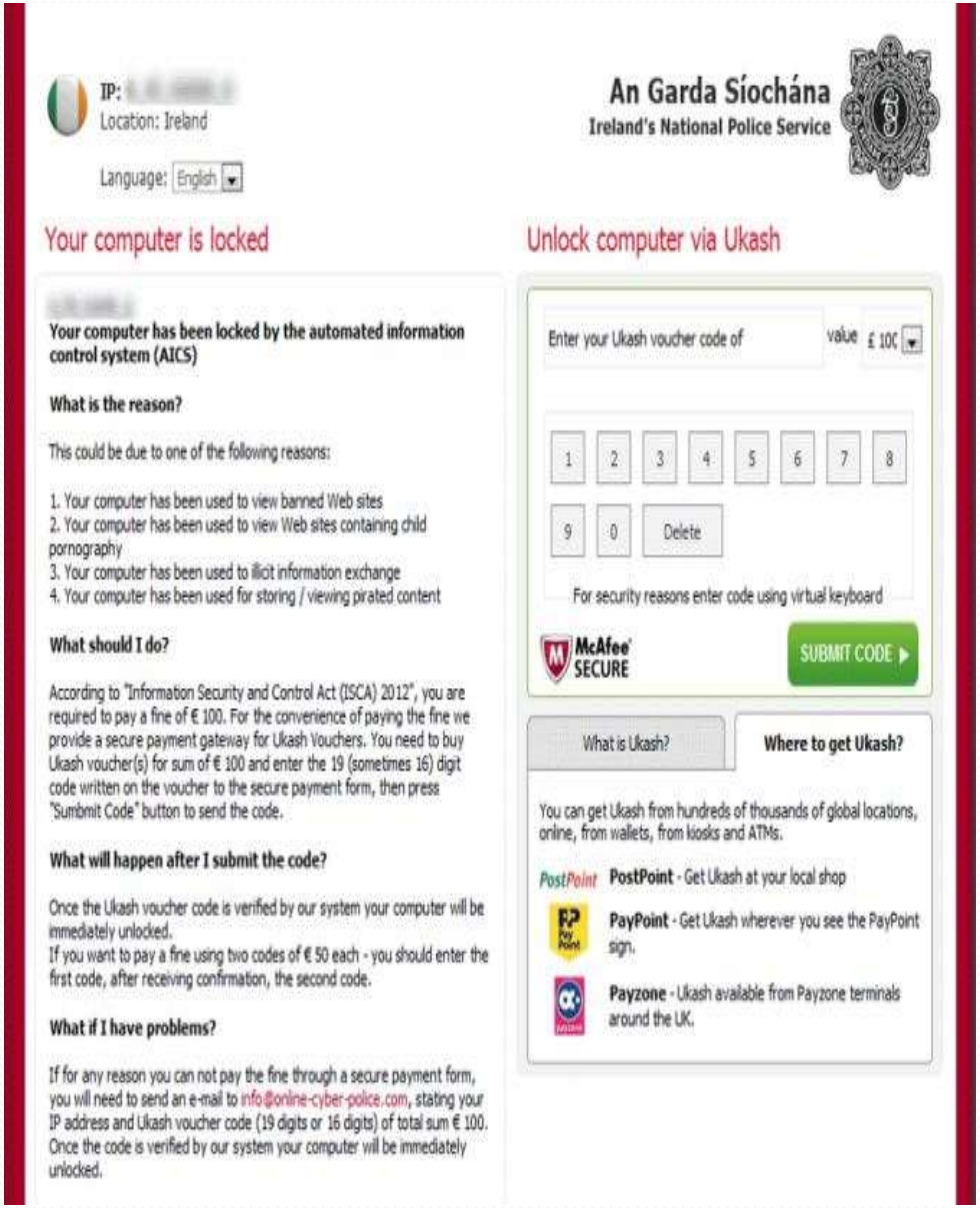


- 30 countries, 100 banks affected

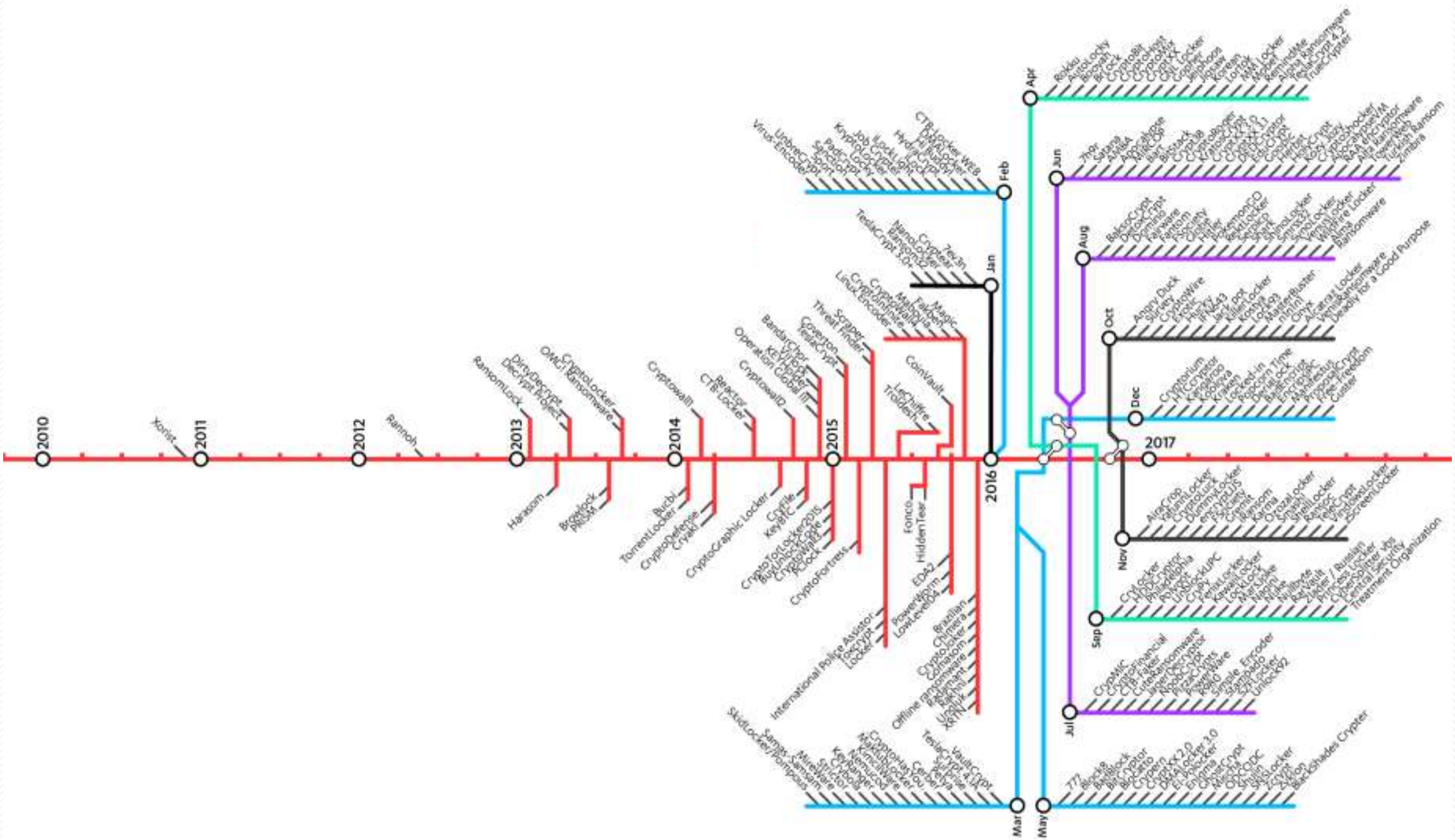
Ransomware

Ransomware

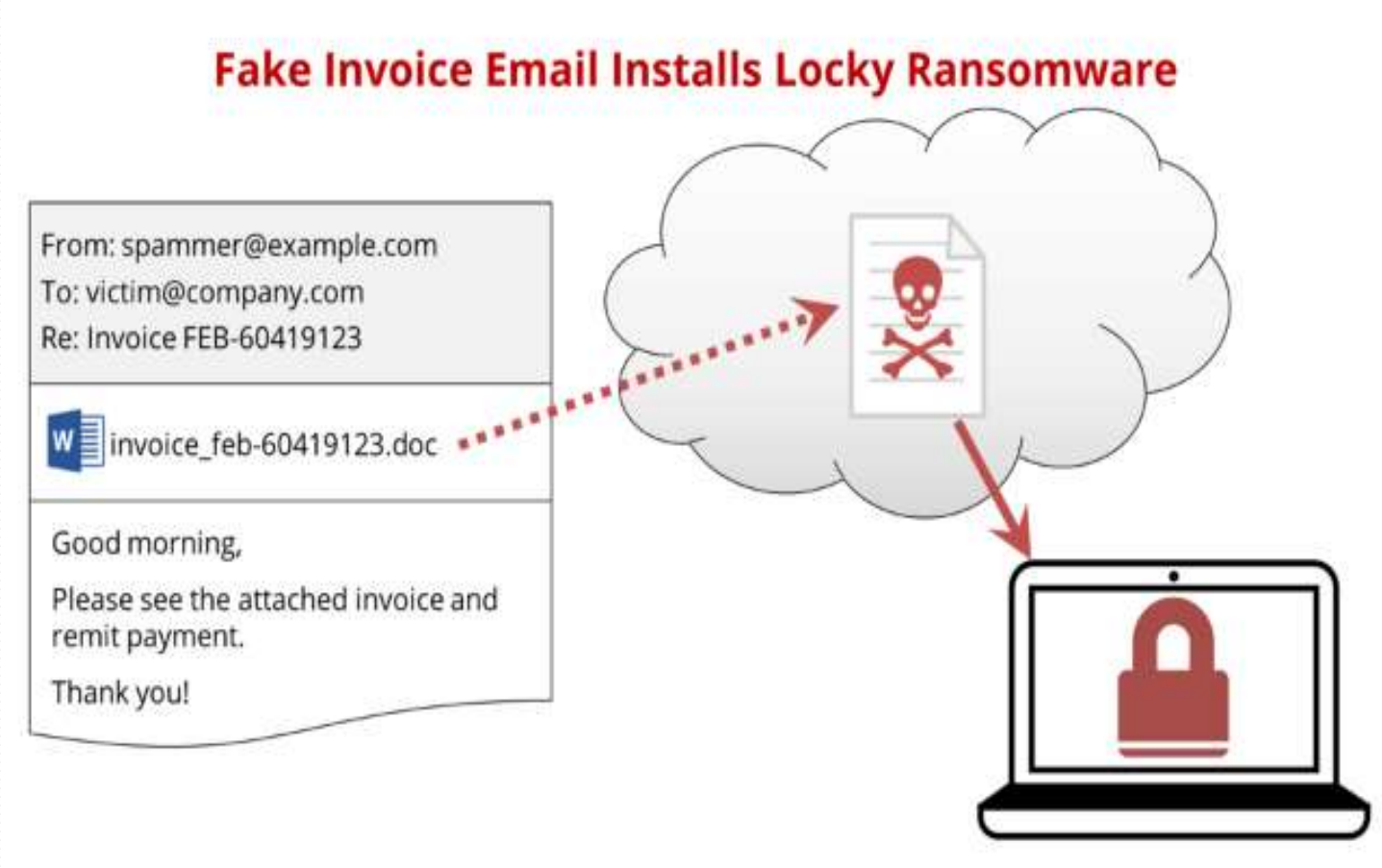
- Ransomware – a type of malware.
- First used 1989 – AIDS Trojan.
- Many different types –Cryptolocker, Locky, Crysis, zCrypt, Powerwave, Petya, HydraCrypt, Cerber, RAA, Cryptowall, Zepto, WannaCry etc.
- Its all about the money! Larger businesses now holding bitcoin as contingency plans.
- “2016 -The year of Ransomware”.
- Ransomware as a service.



Ransomware

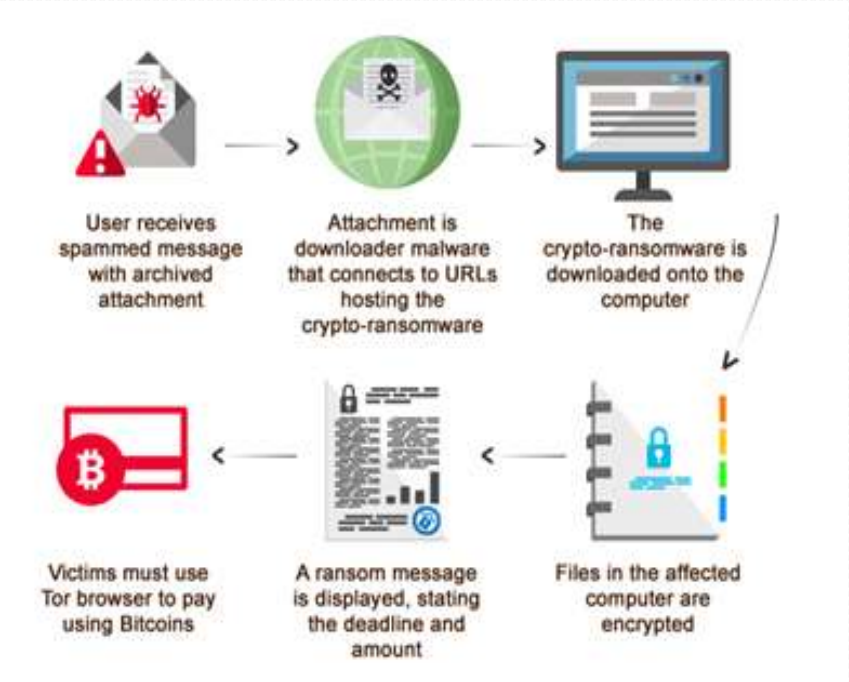


Ransomware


Fake Invoice Email Installs Locky Ransomware
From: spammer@example.com
To: victim@company.com
Re: Invoice FEB-60419123
invoice_feb-60419123.doc
Good morning,
Please see the attached invoice and remit payment.
Thank you!

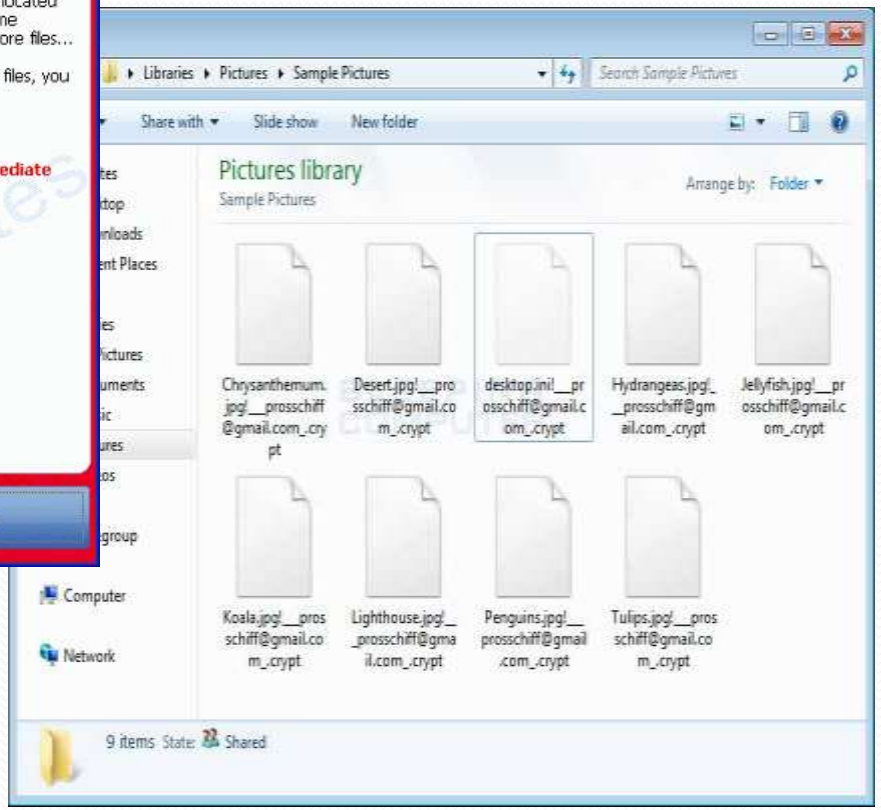
Ransomware

- Ransomware can be installed by accessing a compromised website or opening an attachment in an email.
- After ransomware gets installed it begins encrypting more than 70 types of files that might be present on the victim's device.
- After encrypting the victim's files, the malware sends the encryption key and other host- specific information back to a command-and-control server.
- The server then sends a message to the victim.
- Ransomware can infect any device that the infected computer is connected to i.e. usb stick, other computers, tv, phone.



Ransomware


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35
Next >>


Libraries ▸ Pictures ▸ Sample Pictures
Search Sample Pictures
Share with
Slide show
New folder
Pictures library
Sample Pictures
Arrange by: Folder
Computer
Network
9 items State: Shared

Ransomware

THE IRISH TIMES

Thu, Feb 23, 2017

NEWS SPORT BUSINESS OPINION LIFE & STYLE CULTURE

Technology › How to ... | Data Privacy | Tech Tools

Four in 10 businesses have lost data in cyberattack

RTÉ News Sport Entertainment Business Lifestyle Culture Player TV Radio

News | Ireland World Business Sport Brexit Nuacht Programmes Watch Live

Ransomware 'biggest threat' to cyber security of Irish businesses

Updated / Wednesday, 2 Nov 2016 17:16

PCMag UK | Software Reviews

Maine Police Pay Ransomware Demand in Bitcoin

BY STEPHANIE MLOT 14 APR 2015, 6:55 P.M.

One in five businesses hit by ransomware are forced to close, study shows

Thursday 23 February 2017

News Irish News

Hackers demand €20k as firms hit by 'ransomware'

Irish businesses also targeted by 'garda fine'

RTÉ News Sport Entertainment

News | Ireland World Business

Law firms held to ransom by cyber criminals

Updated / Sunday, 5 Jun 2016 22:16

football opinion culture business lifestyle fashion environment tech travel

Ransomware threat on the rise as 'almost 40% of businesses attacked'

business lifestyle

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Tech Science Magazine

The Oscars 2017 HOW WOULD YOU VOTE?

Technology

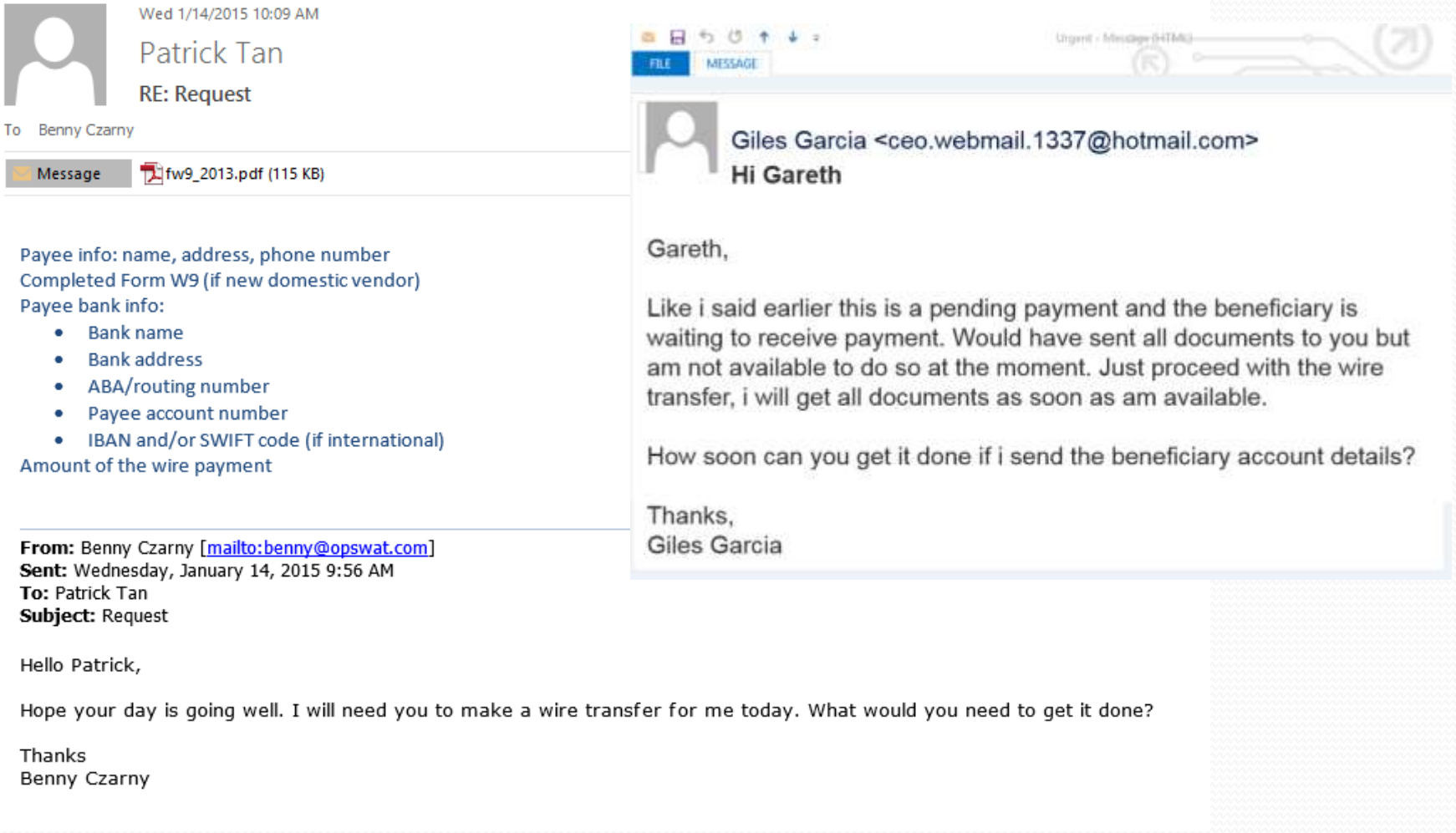
University pays $20,000 to ransomware hackers

Share

Whaling / CEO Fraud

- Purports to be CEO
- Using Executive level email, email spoofed or hacked
- Targeting of unsuspecting employees
- Urgent payment request (outside normal protocols)
- Payment to alternative account
- Funds withdrawn without delay

Whaling / CEO Fraud



Wed 1/14/2015 10:09 AM

Patrick Tan

RE: Request

To Benny Czarny

Message fw9_2013.pdf (115 KB)

Payee info: name, address, phone number
Completed Form W9 (if new domestic vendor)
Payee bank info:

- Bank name
- Bank address
- ABA/routing number
- Payee account number
- IBAN and/or SWIFT code (if international)

Amount of the wire payment

From: Benny Czarny [mailto:benny@opswat.com]
Sent: Wednesday, January 14, 2015 9:56 AM
To: Patrick Tan
Subject: Request

Hello Patrick,

Hope your day is going well. I will need you to make a wire transfer for me today. What would you need to get it done?

Thanks
Benny Czarny

FILE MESSAGE

Giles Garcia <ceo.webmail.1337@hotmail.com>

Hi Gareth

Gareth,

Like i said earlier this is a pending payment and the beneficiary is waiting to receive payment. Would have sent all documents to you but am not available to do so at the moment. Just proceed with the wire transfer, i will get all documents as soon as am available.

How soon can you get it done if i send the beneficiary account details?

Thanks,
Giles Garcia

Whaling / CEO Fraud

May 27, 2016

CEO sacked after aircraft company grounded by whaling attack

Following a successful whaling attack in January which cost FACC €40 million, the company has sacked both its CFO and CEO.

The CEO of an Austrian aircraft parts manufacturer has been sacked after the company lost €40.9 million (£31 million) to a whaling attack.

FINANCIAL TIMES

US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Cyber Security + Add to myFT

CEO email scam costs companies $2bn

07 Tech Firm Ubiquiti Suffers $46M Cyberheist

AUG 15

Networking firm **Ubiquiti Networks Inc.** disclosed this week that cyber thieves recently stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 14, 2016

Alert Number
I-061416-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

News Irish News

Meath Council targeted in 'sophisticated' €4.3m cyber attack

Mark O'Regan and Jim Cusack
December 18 2016 2:30 AM

TCP/IP Attacks

TCP/IP suite controls communication on the Internet. Can be manipulated to prevent users from accessing normal services.

The most common TCP/IP attacks are:

- **Denial of Service (DoS)** - sending enough requests to overload a resource or even stopping its operation.
- **Distributed DoS (DDoS)** - an attack launched from many computers, called **zombies** or **botnets.**
- **SYN Flood -** randomly opens TCP ports at the source of the attack and ties up the computer with a large amount of false SYN requests.
- **Spoofing -** uses a forged IP or MAC address to impersonate a trusted PC.
- **Man-in-the-Middle -** intercepting communications between computers to steal information transiting through the network.
- **Replay -** data transmissions are intercepted and recorded by an attacker, then replayed to gain access.
- **DNS Poisoning -** changing DNS records to point to imposter servers.
- **E-mail Bomb -** is a large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing e-mail

How Bad Can Cyber Attacks Get???

https://www.youtube.com/watch?v=F78UdORll-Q

How Bad Can Cyber Attacks Get???

How Bad Can Cyber Attacks Get???

It is speculated that access to the AP account was gained when a series of “phishing” emails were sent to senior employees. The messages asked recipients to click on a newsworthy link that turned out to be a program that recorded their personal details, including a Twitter account password that was then used to access the feed.

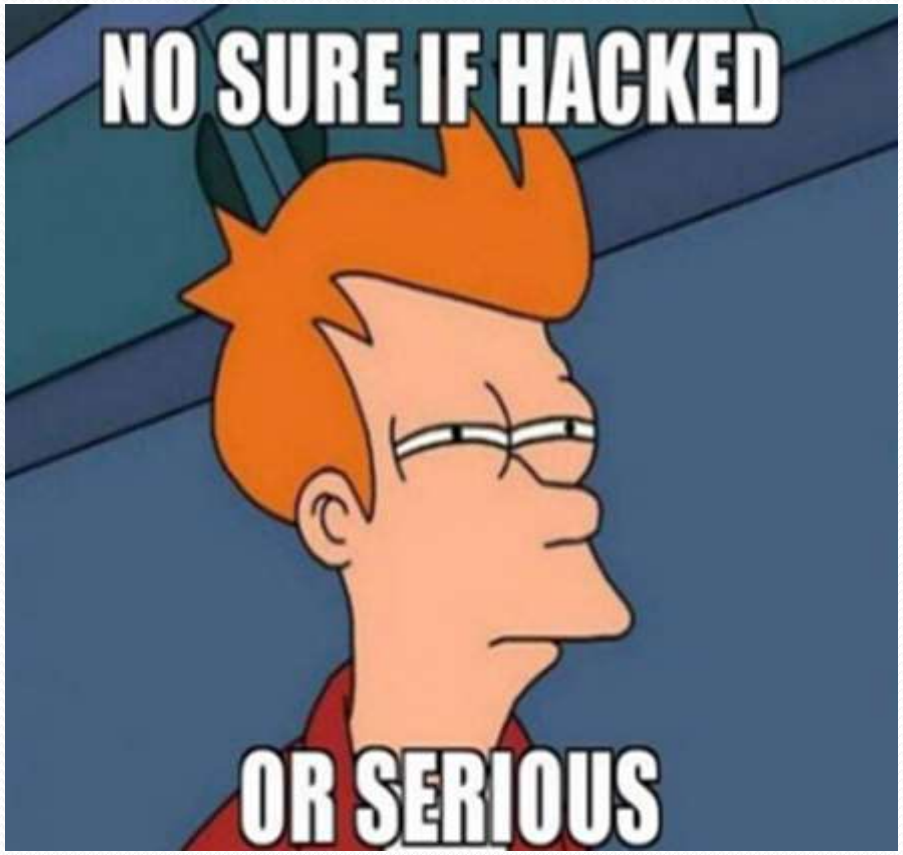
How Bad Can Cyber Attacks Get???

Fooled some news outlets who reported it, sending the Dow Jones plunging 145 points in the space of two minutes — or 1pc.

Wiped out $136.5bn off the index's value in under three minutes.

How Bad Can Cyber Attacks Get???

How Bad Can Cyber Attacks Get???



Why Can’t We Police It???

Why Can’t We Police It???

- Jurisdiction : Most of the time the people involved are outside of the country.
- Requires cooperation from several police forces from different country’s to trace.
- Hackers are very good at covering their steps (hide and seek champions!!).
- Some companies don’t want to disclose a breach, for fear of shaking consumer and investor confidence and to protect its brand.
- Can be very hard to prove. Hackers may delete or encrypt evidence.

Social Media Concerns

- Viruses via Messaging systems
- Leak of Sensitive Data
- Personal Data Being Used For Targeted Attacks
- Privacy Implications
- Hijacking of Corporate Social Media Accounts
- Inappropriate Updates from Corporate Social Media Accounts
- Fake News/Updates
- GEO Tagging

Protecting Data

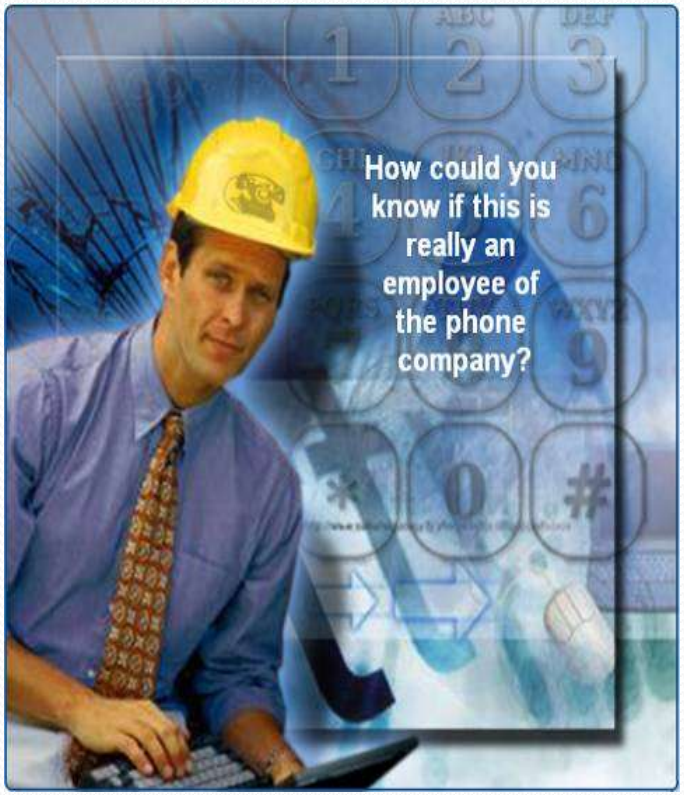
The value of physical equipment is often far less than the value of the data it contains. To protect data, there are several methods of security protection that can be implemented.

Depending on the situation, more than one technique may be required:

- Password protection
- User accounts
- File system security
- Data encryption
- Data backups
- Firewalls
- Updates
- Access Control Devices

Social Engineering

- A **social engineer** is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information.
- To protect against social engineering:
  - Never give out a password.
  - Always ask for the ID of the unknown person.
  - Restrict access of visitors.
  - Escort all visitors.
  - Never post your password.
  - Lock your computer when you leave your desk.
  - Do not let anyone follow you through a door that requires an access card.



Protecting Data

- The value of physical equipment is often far less than the value of the data it contains. To protect data, there are several methods of security protection that can be implemented.
  - **Password protection** can prevent unauthorised access to content. Password policies should include:
    - Expire after a set period of time, Contain a mixture of letters and numbers, Prevent users from leaving written passwords in view, Lockout rules to limit the number of unsuccessful attempts
  - **Data encryption** uses codes and ciphers. Virtual Private Network (VPN) uses encryption to protect data. A VPN connection allows a remote user to safely access resources as if their computer is physically attached to the local network.
  - **Firewall** Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A firewall is a way of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured.

Protecting Data

- **Data backups** are one of the most effective ways of protecting against data loss. Establish data backup procedures which account for frequency of backups, storage for data backups, and securing data backups using passwords.
- **Smart Card Security** Smart cards store private information such as bank account numbers, personal identification, medical records, and digital signatures. Smart cards provide authentication and encryption to keep data safe.
- **Biometric Security** compares physical characteristics against stored profiles to authenticate people. A profile is a data file containing known characteristics of an individual such as a fingerprint or a handprint. Common biometric devices available include fingerprint readers, handprint readers, iris scanners, and face recognition devices.
- **File system security** All file systems keep track of resources, but only file systems with journals can log access by user, date, and time. The FAT 32 file system lacks both journaling and encryption capabilities. As a result, situations that require good security are usually deployed using a file system such as NTFS.

Password Requirements

Guidelines for creating strong passwords:

- **Length -** Use at least eight characters.
- **Complexity -** Include letters, numbers, symbols, and punctuation. Use a variety of keys on the keyboard, not just common letters and characters.
- **Variation -** Change passwords often. Set a reminder to change the passwords you have for email, banking, and credit card websites on the average of every three to four months.
- **Variety** - Use a different password for each site or computer that you use.

Password Guide

- Make your password impossible to guess. It's an obvious one but change to something more complex. Hackers have programs at their disposal that within seconds try all the words in the dictionary.
- Never save your passwords on computers you share, or mobile devices that can easily be lost or stolen.
- Always log out from mobile devices. With most apps having one click log in without the need to put any info, it's never been easier to get in the possession of someone's social media account. It may take as much as leaving your mobile unattended whilst going to the toilet to lose the ownership of your account for good.
- Never store passwords on a post-its, spread sheets or in email.
- Have a limited number of employees accessing your company's Twitter account. Social media has gone mainstream, and sometimes the whole team from interns to top execs have the access to the corporate Twitter, Facebook or even LinkedIn account.
- Don't click on links in emails that tell you to change your account for any social media platform.

Password Guide

- Use an “https” addresses for extra layer of protection.
- Turn your Twitter settings to login approval in order to encrypt and protect your activity and prevent outside sources from accessing your account without your permission.
- Every message you receive on Twitter or Facebook, LinkedIn and any other social platform should be scrutinised. Is the source / sender likely to message you? In addition, check if it’s grammatically correct. Hacked messages often contain strange errors that may seem out of place – that’s because they are. In most cases the message will try to urge you to click on the link to see supposedly hilarious picture of you or read about the gossip that someone is allegedly spreading. Delete the message instantly, without clicking on the said link.
- Be cautious when receiving shortened links, especially from accounts you don’t know well. Hackers often use those links to drive you to malicious websites.
- Be cautious when granting permission to third party apps and review the permissions granted regularly. Remove the access to your accounts from apps you no longer use.

Password Cracking

6 characters: 2.25 billion possible combinations

- Cracking online using web app hitting a target site with one thousand guesses per second: 3 weeks.
- Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 0.0224 seconds
- Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 0.0000224 seconds

Password Cracking

10 characters: 3.76 quadrillion possible combinations

- Cracking online using web app hitting a target site with one thousand guesses per second: 7 weeks.
- Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 10.45 hours
- Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 37.61 seconds.

Password Cracking

Add a symbol, make the crack several orders of magnitude more difficult:

6 characters: 7.6 trillion possible combinations

- Cracking online using web app hitting a target site with one thousand guesses per second: 2.4 centuries.
- Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 1.26 minutes
- Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 0.0756 seconds

Password Cracking

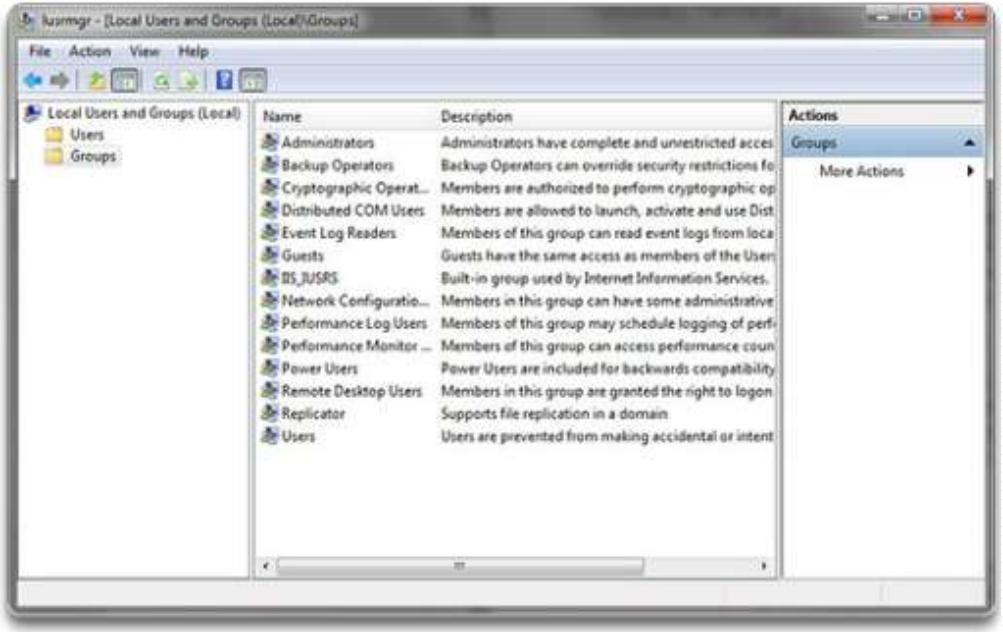
Add a symbol, make the crack several orders of magnitude more difficult:

10 characters: Possible combinations: 171.3 sextillion (171,269,557,687,901,638,419; 1.71 x 1020)

- Cracking online using web app hitting a target site with one thousand guesses per second: 54.46 million centuries.
- Cracking offline using high-powered servers or desktops (one hundred billion guesses/second) 54.46 years
- Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 2.83 weeks.

Maintaining Accounts

- When an employee leaves an organisation, access to the network should be terminated immediately.
- Guests can be given access through a Guest account.
- Keep control over who has an account.



Data Encryption

- Encryption - data is transformed using a complicated algorithm to make it unreadable.
- **Encrypting File System (EFS)** is a Windows feature that can encrypt data.
- **BitLocker** can encrypt the entire hard drive volume included in Windows 10/8/7 and Windows Vista Ultimate and Enterprise editions.
- **TrueCrypt** is a free open-source disk encryption software for Windows 10/8/7/Vista/XP, Mac OS X, and Linux.

  Replaced by CipherShed and VeraCrypt

Simple Encryption Example

Caesar cipher, each character of the plain text (plain text is the message which has to be encrypted) is substituted by another character to form the cipher text (cipher text is the encrypted message). The variant used by Caesar was a shift by 3 cipher. Each character was shifted by 3 places, so the character ‘A’ was replaced by ‘D’, ‘B’ was replaced by ‘E’, and so on. The characters would wrap around at the end, so ‘X’ would be replaced by ‘A’.

$$c_i = E(p_i) = p_i + 3$$

A full translation chart of the Caesar cipher is shown here.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

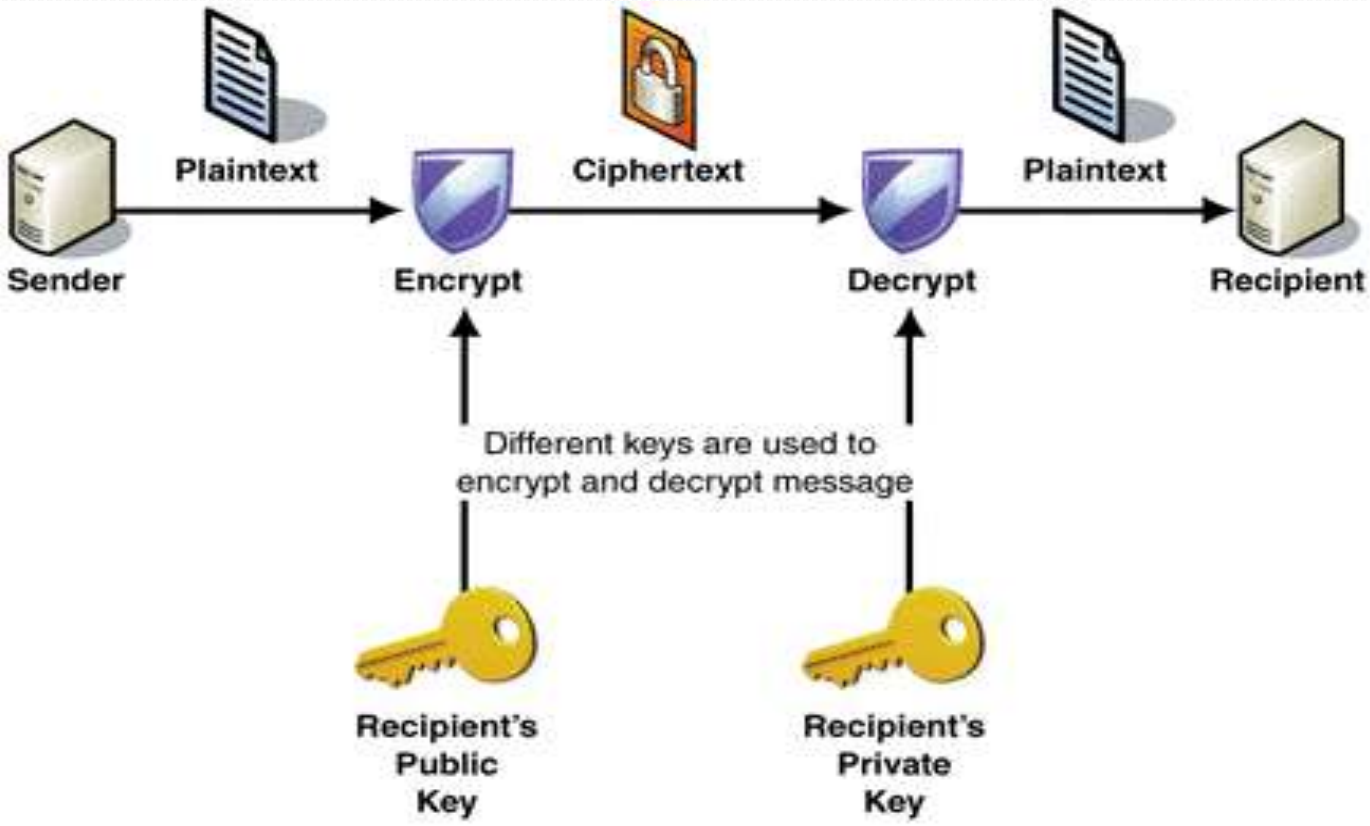
Using this encryption, the message

TREATY IMPOSSIBLE

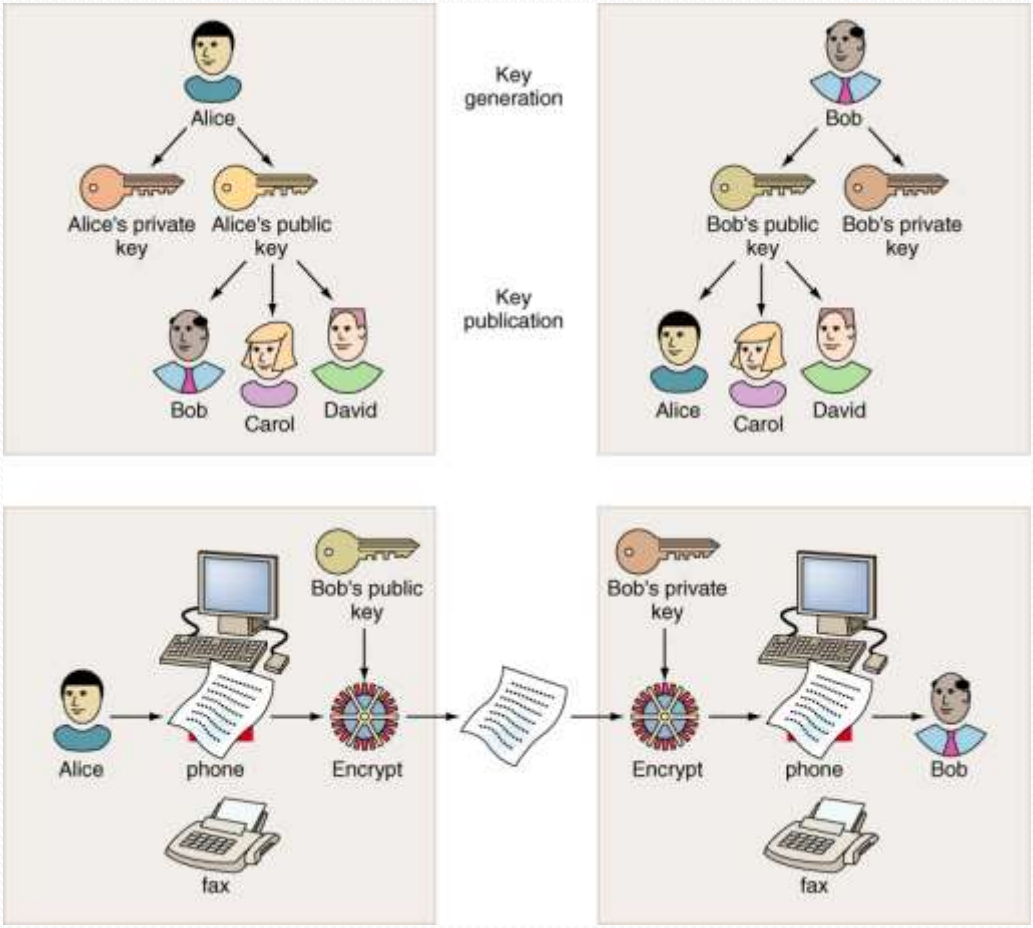
would be encoded as

T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

How Public Key Encryption Works



How Public Key Encryption Works



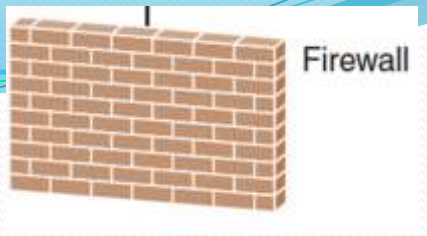
Hard Drive Disposal and Recycling

- Erase all hard drives, then use a third-party data wiping tool to fully erase all data.
- Degaussing disrupts or eliminates the magnetic field on a hard drive that allow for the storage of data. A degaussing tool is very expensive and not practical for most users.
- **The only way to fully ensure that data cannot be recovered from a hard drive is to carefully shatter the platters with a hammer and safely dispose of the pieces.**
- To destroy software media (floppy disks and CDs), use a shredding machine designed for shredding these materials.
- **Hard Drive Recycling -** Hard drives that do not contain sensitive data can be reformatted and used in other computers.

Data Backup

- A data backup stores a copy of the information on a computer to removable backup media that can be kept in a safe place. If the computer hardware fails, the data backup can be restored so that processing can continue.
- Backups can be done manually or scheduled to takes place automatically.
- Data backups should be performed on a regular basis.
- If possible always have a backup locked away, or have a backup offsite.
- Backup your backup!!!

Firewalls



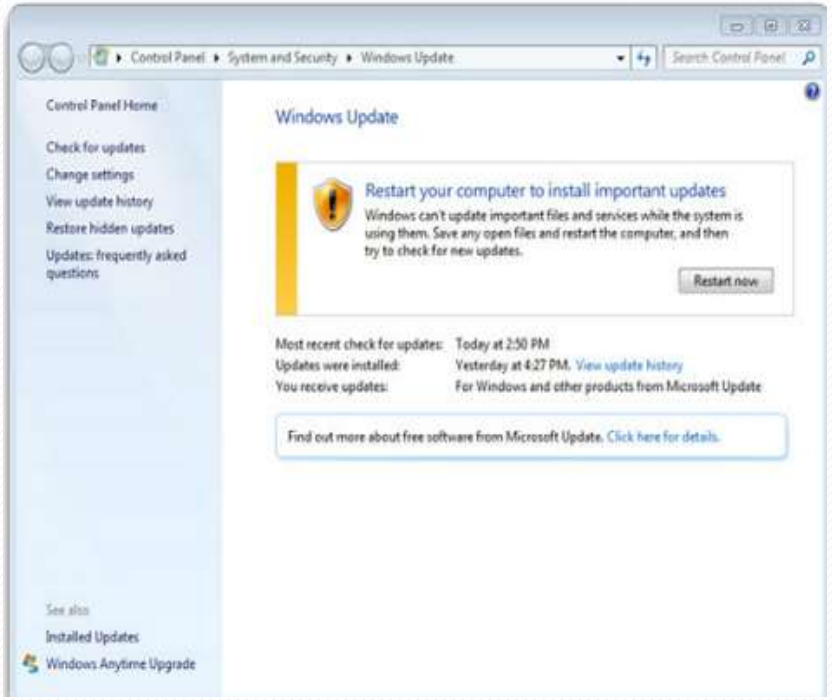
A hardware firewall is a physical filtering component that inspects data packets from the network before they reach computers and other devices on a network. Hardware firewalls are often installed on routers. A hardware firewall is a free-standing unit that does not use the resources of the computers it is protecting, so there is no impact on processing performance.

A software firewall is an application on a computer that inspects and filters data packets. A software firewall uses the resources of the computer, resulting in reduced performance for the user.

Hardware Firewall	Software Firewall
Dedicated hardware component	Available as third-party software, cost varies
Initial cost for hardware and software updates can be expensive	Free version included with Windows operating system
Multiple computers can be protected	Typically protects only the computer on which it is installed
No impact on computer performance	Uses the CPU, potential impact on computer performance

Service Packs and Security Patches

- Regular security updates are essential to combat new viruses or worms.
- **Patches** are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack
- A **Service Pack** is a combination of patches and updates.



Physical Access Control Devices

- Physical access control devices
  - Lock
  - Card key
  - Video surveillance
- Two-factor identification methods for access control (use both a password and a data security device)
  - Smart card
  - Security key fob
  - Biometric device

Physical Access Control Devices

Physical access control devices are used to secure access to data and equipment by physical means.

- A lock is the most common device for securing physical areas. If a key is lost, all identically keyed locks must be changed.
- A card key is a tool used to secure physical areas. If a card key is lost or stolen, only the card must be deactivated. The card key is more expensive than security locks.
- Video surveillance equipment records images and sound for monitoring activity. The recorded data must be monitored for problems.
- Security guards control access to the entrance of a facility and monitor the activity inside the facility.

Access Control Devices

Data security devices are used to authenticate employees and authorised personnel to access to data on a computer and on a network. Two-factor identification is a method to increase security. Employees must use both a password and a data security device similar to those listed here to access data:

- Smart card is a device that has the ability to store data safely. The internal memory is an embedded integrated circuit chip (ICC) that connects to a reader either directly or through a wireless connection. Smart cards are used in many applications worldwide, like secure ID badges, online authentication devices, and secure credit card payments.
- Security key fob is a small device that resembles the ornament on a key ring. It has a small radio system that communicates with the computer over a short range. The fob is small enough so that many people attach them to their key rings. The computer must sense the signal from the key fob before it will accept a username and password.
- A biometric device measures a physical characteristic of the user, such as their fingerprints or the patterns of the iris in the eye. The user will be granted access if these characteristics match its database and the correct login information is supplied.

Physical Equipment Protection Methods

- Since stealing the whole PC is the easiest way to steal data, physical computer equipment must be secured.
- Physical security is as important as data security. Network infrastructure can be protected by:
  - Secured telecommunications rooms, equipment cabinets, and cages
  - Cable locks and security screws for hardware devices
  - Wireless detection for unauthorised access points
  - Hardware firewalls
  - Network management system that detects changes in wiring and patch panels
- **Two- factor Authentication -** secured using overlapping protection techniques to prevent unauthorised access to sensitive data.
  - An example of two-factor authentication is using a password and a smart card to protect an asset.

Security Hardware

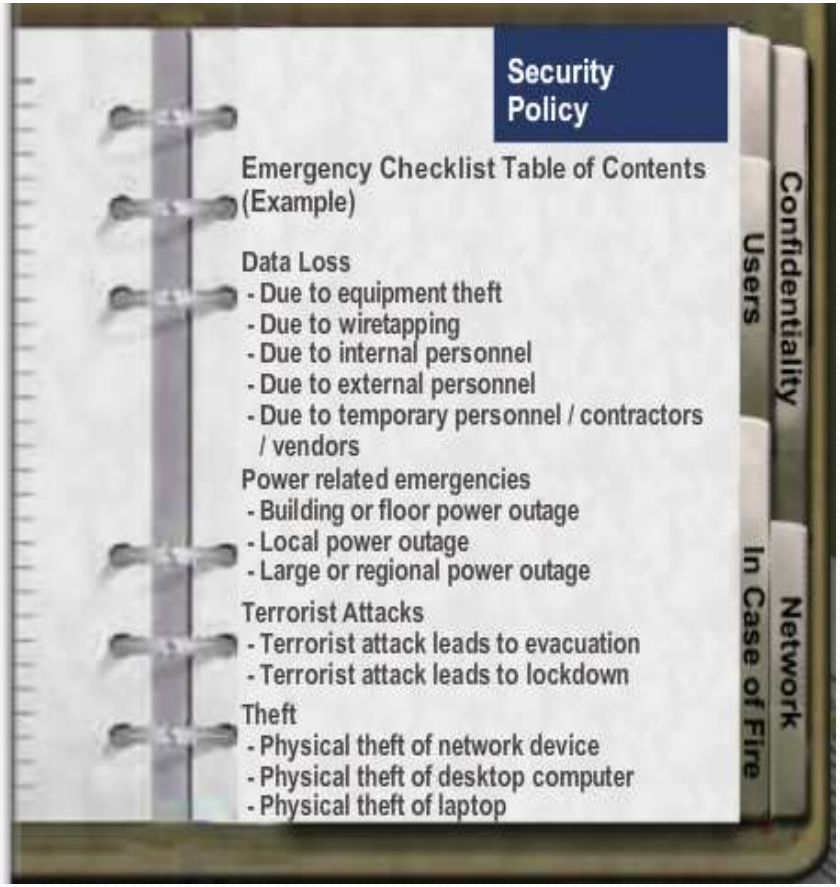
- There are several methods of physically protecting computer equipment:
  - Use cable locks with equipment.
  - Keep telecommunication rooms locked.
  - Fit equipment with security screws.
  - Use security cages around equipment.
  - Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment.
  - Install physical alarms triggered by motion-detection sensors.
  - Use webcams with motion-detection and surveillance software.
- For access to facilities, there are several means of protection:
  - Card keys that store user data, including level of access
  - Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
  - Posted security guard
  - Sensors, such as RFID tags, to monitor equipment

Security Policy

- A security policy should describe how a company addresses security issues

- Questions to answer in writing a local security policy:

  - What assets require protection?
  - What are the possible threats?
  - What should be done in the event of a security breach?
  - What training will be in place to educate the end users?



Outline Security Requirements

- An organisation should strive to achieve the best and most affordable security protection against data loss or damage to software and equipment.
- A security policy includes a comprehensive statement about the level of security required and how this security will be achieved.
  - Is the computer located at a home or a business?
  - Is there full-time Internet access?
  - Is the computer a laptop?

Security Policy Requirements

A security policy should address these key areas:

- Process for handling network security incidents
- Process to audit existing network security
- General security framework for implementing network security
- Behaviors that are allowed
- Behaviors that are prohibited
- What to log and how to store the logs: Event Viewer, system log files, or security log files
- Network access to resources through account permissions
- Authentication technologies to access data: usernames, passwords, biometrics, and smart cards

Outline a Security Policy

- **A Security Policy is a collection of rules, guidelines, and checklists:**
  - Identify the people permitted to use the computer equipment.
  - Identify devices that are permitted to be installed on a network, as well as the conditions of the installation.
  - Define the requirements necessary for data to remain confidential on a network.
  - Determine a process for employees to acquire access to equipment and data.
  - Define an acceptable computer usage statement.

- **The security policy should also provide detailed information about the following issues in case of an emergency:**
  - Steps to take after a breach in security
  - Who to contact in an emergency
  - Information to share with customers, vendors, and the media
  - Secondary locations to use in an evacuation
  - Steps to take after an emergency is over, including the priority of services to be restored

Leading Practises

Increasing Impact