Cybercrime

Cybercrime at a glance

- **Cybercrime**
  - Illegal activity conducted on a computer
  - The computer is either a **tool**, or a **target**, or both

- **Cyberlaw**
  - Area of law dedicated to cybercrime
  - Under developed or difficult to enforce in some countries
    - Ex: Love Bug Virus
    - Corrupting VB script that spread over email
    - Created in the Philippines

Types and tools of cybercrime

- Viewing or purchasing illegal content/merchandise
- Identity theft
- Cyberbullying and cyberstalking
- Phishing attacks
- Pharming
- Spam
- **Malware**: malicious code or software designed to damage, disrupt, steal or negatively affect data, hosts, or networks
- Botnets
- Denial of Service (DOS) attacks

Phishing attacks

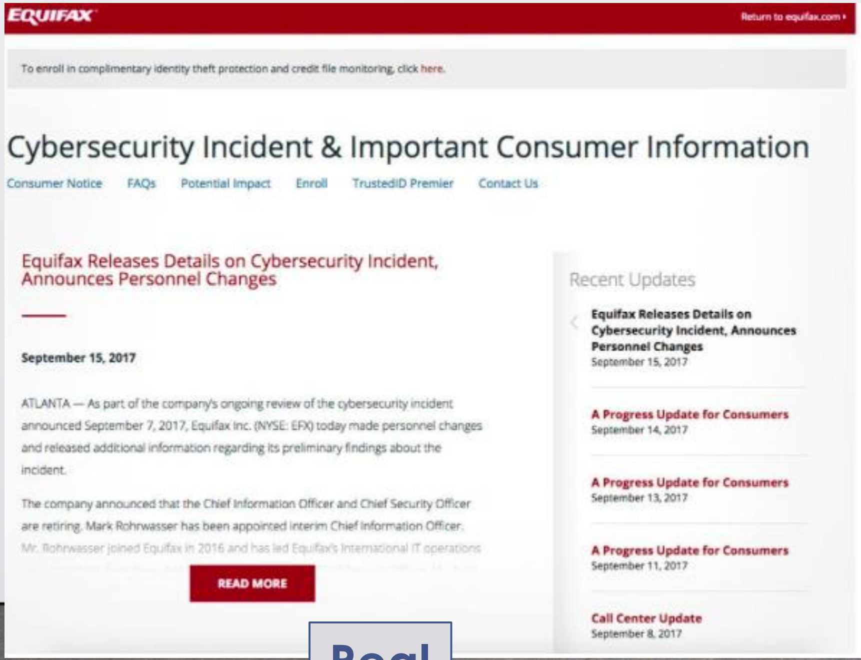
- **Phishing**
  - An attempt to obtain sensitive information by disguising as a trustworthy entity
  - Often used get sensitive information or download malware
  - Example: click on a URL or open attachment
  - **Spear Phishing**: designed for a specific individual or organization
  - **Whaling**: targeted at executive-level individuals

How to protect yourself

- Be suspicious of links and attachments
- Check spelling of URLs and emails
- Contact supposed source of email with a new email (don’t hit reply)
- Don’t post personal data publicly

Pharming

- **Pharming**
  - Fake website collects data you intended for real website
  - Can redirect requests for real website to the fake one
- Example
  - Fake Equifax site linked to by Equifax



To enroll in complimentary identity theft protection and credit file monitoring, click here.

Cybersecurity Incident & Important Consumer Information

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

September 15, 2017

ATLANTA — As part of the company's ongoing review of the cybersecurity incident announced September 7, 2017, Equifax Inc. (NYSE: EFX) today made personnel changes and released additional information regarding its preliminary findings about the incident.

The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations

Recent Updates

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes
September 15, 2017

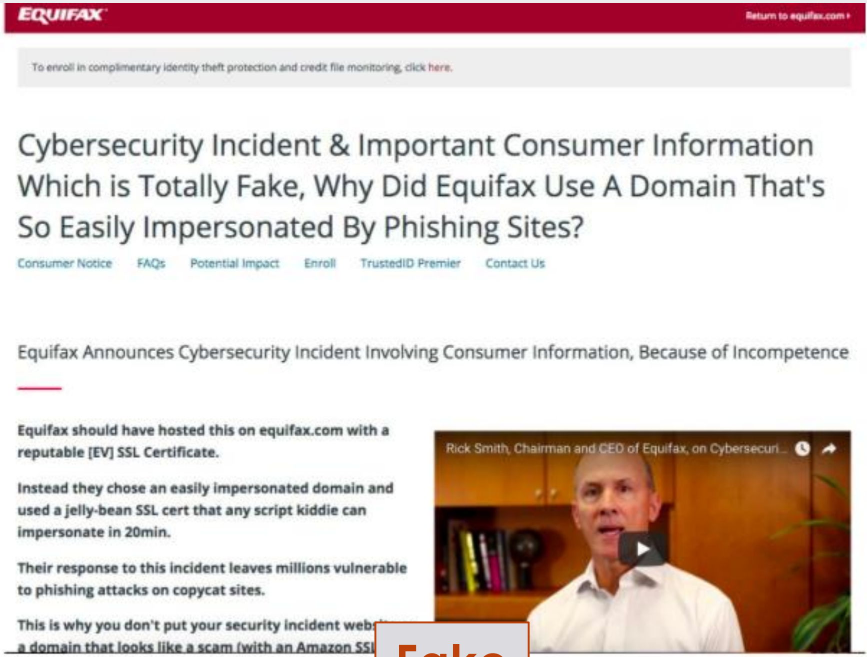
A Progress Update for Consumers
September 14, 2017

A Progress Update for Consumers
September 13, 2017

A Progress Update for Consumers
September 11, 2017

Call Center Update
September 8, 2017

Real



To enroll in complimentary identity theft protection and credit file monitoring, click here.

Cybersecurity Incident & Important Consumer Information Which is Totally Fake, Why Did Equifax Use A Domain That's So Easily Impersonated By Phishing Sites?

Equifax Announces Cybersecurity Incident Involving Consumer Information, Because of Incompetence

Equifax should have hosted this on equifax.com with a reputable [EV] SSL Certificate.

Instead they chose an easily impersonated domain and used a jelly-bean SSL cert that any script kiddie can impersonate in 20min.

Their response to this incident leaves millions vulnerable to phishing attacks on copycat sites.

This is why you don't put your security incident web a domain that looks like a scam (with an Amazon SSL

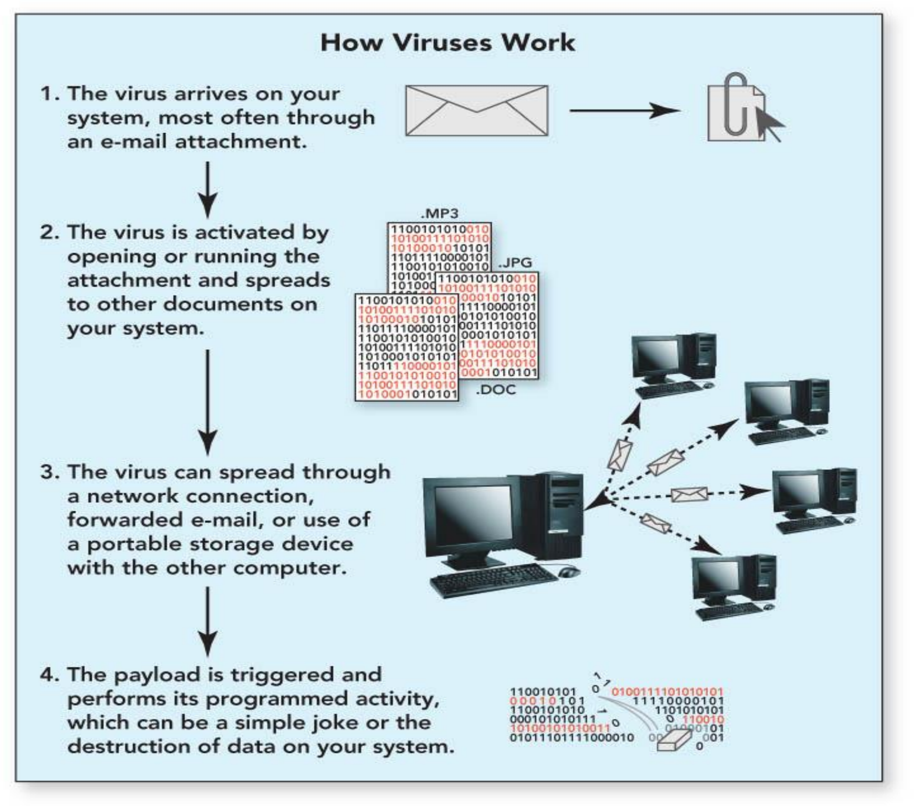
Fake

Spam

- **Spam**
  - Mass distribution of unsolicited messages
  - Often used for phishing
  - Vehicle for malware, scams, and fraud
- 85% of all email traffic in 2016
- Majority comes from the US
- Burdens communication service providers

Malware: Computer Virus

- **Computer Virus**
  - Software capable of replicating itself by modifying other programs and inserting its own code
  - Spread to other systems by people
  - Often used for ransom, monitoring, control, or corrupting data



How Viruses Work

1. The virus arrives on your system, most often through an e-mail attachment.
2. The virus is activated by opening or running the attachment and spreads to other documents on your system.
3. The virus can spread through a network connection, forwarded e-mail, or use of a portable storage device with the other computer.
4. The payload is triggered and performs its programmed activity, which can be a simple joke or the destruction of data on your system.

Examples

- Pikachu virus can delete all system files on restart
- Shamoon uploads files to the attacker, erases them, and bricks the computer

Malware: Computer Worms

- **Computer Worm**
  - Standalone program that replicates itself using a computer network
  - Doesn’t need human help to propogate
  - Often used for ransom, monitoring, control, or corrupting data

- Examples
  - Stuxnet specifically targeted Iran’s nuclear program, disrupted centrifuges
  - ILOVEYOU stole login credentials
  - Morris Worm intended to gauge the size of the internet, but made infected computers more susceptible

Malware: Trojan

- **Trojan**
  - Harmful software typically hidden in a legitimate-looking program
  - Doesn't propagate
  - Often used for ransom, monitoring, control, backdoor access, or corrupting data

- Examples
  - Zeus is used to steal banking information with keystroke logging
  - Sakula RAT (remote access Trojan) affected the Office of Personnel Management (OPM)
  - Rogue security software: malicious fake software

AntiVirus 360
ContraVirus
MacSweeper
Spyware Quake
SpywareStrike
UltimateCleaner
WinAntiVirus Pro 2006
Windows Police Pro

Malware: Ransomware

- **Ransomware**
  - A type of malware that threatens to publish the victim's data or block access to it unless a ransom is paid

- Examples:
  - First attack in 1989, AIDS Trojan asked users to pay $189 for an expired license. Attacker promised to donate profits to AIDS research
  - WannaCry shut down hospital infrastructure in the UK

Malware: Spyware

- **Spyware**
  - Obtain information from the user without their knowledge and transmits it
  - Runs in the background to collect information and monitor
  - Can slow down your computer
  - Can come from a malicious site or be included with genuine software
  - **Adware**: any software that tracks your internet browsing habits to send you related ads
- Examples
  - Kazaa shipped with spyware included
  - Weatherbug is a weather app which also keeps tracking data
  - Rogue security software

How to protect yourself from malware

- Anti-malware software
- Use a firewall
- Don’t open emails or attachments from unknown senders
- Think before you click on popups
- Download software from official websites
- Beware of free software

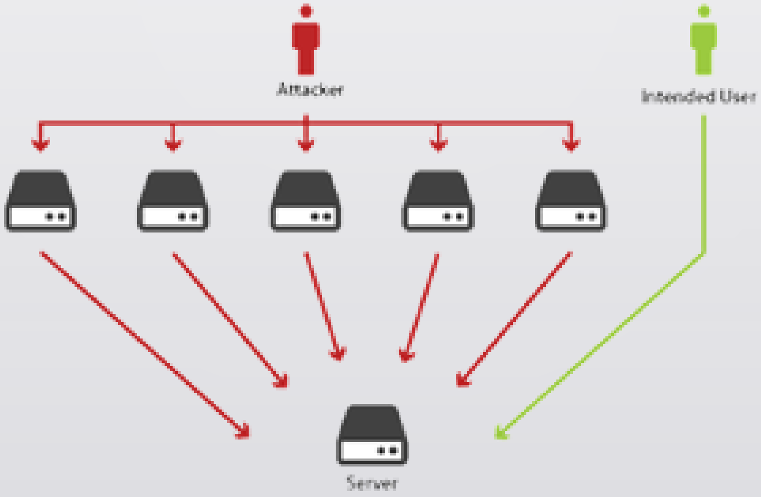
Botnets

- **Botnet**
  - A network of computers infected with malware and controlled as a group without the owner's knowledge
  - Often used to
    - send spam with viruses
    - spread malware
    - use your computer as part of a DoS attack

Denial of Service Attack

DOS Attack

- Render a machine or service unavailable by flooding it with illegitimate requests
- **Distributed DOS (DDoS) attack**: incoming traffic comes from many different sources
  - Many recent DDoS attacks use a **Mirai botnet** that targets IoT devices


Attacker
Intended User
Server