CY 2550 Foundations of Cybersecurity

Cyberlaw

Learning Outcomes

Cryptography, passwords, and authentication

- Exercised your password cracking skills

Vulnerabilities and exploits

- Practice performing live exploits

Cybercrime underground

- How the criminals make money

Cybersecurity is A Fraught Subject

- Many laws govern cybersecurity
  - Designed to help prosecute criminals
  - Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
  - Easy to violate these laws accidentally
  - Security professionals must be cautious and protect themselves

Cybersecurity is A Fraught Subject

- Many laws govern cybersecurity
  - Designed to help prosecute criminals
  - Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
  - Easy to violate these laws accidentally
  - Security professionals must be cautious and protect themselves
- Cybersecurity raises complex ethical questions
  - When and how to disclose vulnerabilities
  - How to handle leaked data
  - Line between observing and enabling crime
  - Balancing security vs. autonomy

Cybersecurity is A Fraught Subject

- Many laws govern cybersecurity
  - Designed to help prosecute criminals
  - Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
  - Easy to violate these laws accidentally
  - Security professionals must be cautious and protect themselves
- Cybersecurity raises complex ethical questions
  - When and how to disclose vulnerabilities
  - How to handle leaked data
  - Line between observing and enabling crime
  - Balancing security vs. autonomy
- Ethical norms must be respected
  - Rights and expectations of individuals and companies
  - Community best-practices

Legal != Ethical

Illegal != Unethical

Cyberlaw

Computer Fraud and Abuse Act (CFAA) of 1986

Digital Millennium Copyright Act (DMCA) of 1998

CAN-SPAM Act of 2003

Disclaimer: I am not a lawyer, and nothing in this lecture should be construed as legal advice.

If you believe you may be at legal risk, seek advice from a lawyer.

- Grey hat hacking: Electronic Frontier Foundation (eff.org)
- Privacy and surveillance: Electronic Privacy Information Center (epic.org)

How Are Cybercriminals Prosecuted?

Pyotr Levashov, a.k.a. Severa

Highly prolific spammer for SpamIt pharma affiliate program

Moderator of spamdot.biz

Possible operator of the Storm, Waledac, and Kelihos botnets

Pyotr Levashov, a.k.a. Severa

Highly prolific spammer for SpamIt pharma affiliate program

Moderator of spamdot.biz

Possible operator of the Storm, Waledac, and Kelihos botnets

Arrested in Barcelona in April 2017

Extradited to the US in Feb 2018

Charges Against Severa

1. One count of causing intentional damage to a protected computer
2. One count of accessing protected computers in furtherance of fraud
3. One count of threatening to damage a protected computer
4. One count of conspiracy
5. One count of wire fraud
6. Two counts of fraud in connection with email
7. One count of aggravated identity theft

Charges Against Severa

1. One count of causing intentional damage to a protected computer
2. One count of accessing protected computers in furtherance of fraud
3. One count of threatening to damage a protected computer
4. One count of conspiracy
5. One count of wire fraud
6. Two counts of fraud in connection with email
7. One count of aggravated identity theft

CFAA

Charges Against Severa

1. One count of causing intentional damage to a protected computer
2. One count of accessing protected computers in furtherance of fraud
3. One count of threatening to damage a protected computer
4. One count of conspiracy
5. One count of wire fraud
6. Two counts of fraud in connection with email
7. One count of aggravated identity theft

CFAA

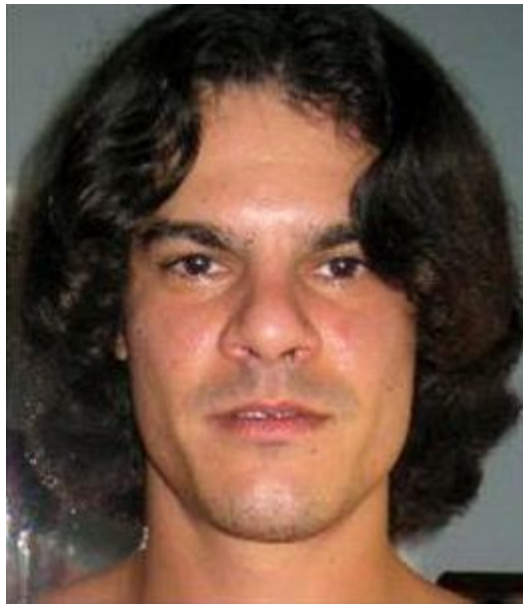
CAN-SPAM Act

Albert Gonzalez

Led hacks against TJ Maxx, Heartland Payment Systems, 7-Eleven, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority

TJX hack netted 94 million stolen credit cards

Caught and sentenced to 20 years in March 2010



Charges Against Gonzalez

1. Conspiracy
2. Wire fraud
3. Aggravated identity theft
4. Computer fraud
5. Access device fraud

Marcus Hutchins, aka malwaretech

Anti-malware researcher

Accidentally stopped the WannaCry malware outbreak

Marcus Hutchins, aka malwaretech

Anti-malware researcher

Accidentally stopped the WannaCry malware outbreak

Arrested in August 2017

Accused of writing, selling, and possibly operating the Kronos banking trojan

Charges Against malwaretech

Original charges

- One count of conspiracy
- One count of causing intentional damage to a protected computer
- Four counts of illegal wiretapping

Bonus charges!

- Lying to federal investigators
- CFAA violations for writing malware
- Contributory CFAA violations for selling malware
- Wiretapping

Marcus Hutchins, aka malwaretech

Marcus Hutchins, aka malwaretech

Anti-malware researcher

Accidentally stopped the WannaCry malware outbreak

Arrested in August 2017

Accused of writing, selling, and possibly operating the Kronos banking trojan

Plead guilty to a reduced count of charges in 2019, sentenced to time served (~2 years)

Computer Fraud and Abuse Act of 1986

(Supposedly) written and enacted in response to the movie WarGames

Prohibits **accessing a protected computer without authorization**, or in excess of authorization

Provides civil and criminal penalties

CFAA Details

What is a “protected computer”?

- “[Any computer] used in or affecting interstate or foreign commerce or communication”
- Essentially, any computer connected to the internet

CFAA Details

What is a “protected computer”?

- “[Any computer] used in or affecting interstate or foreign commerce or communication”
- Essentially, any computer connected to the internet

Criminal offenses

- Unauthorized access to information on a protected computer
- Leveraging unauthorized access to commit fraud for something of value worth >$5000
- Causing damage or loss to a protected computer
- Threatening to cause damage to or steal information from a protected computer without authorization

CFAA Details

What is a “protected computer”?

- “[Any computer] used in or affecting interstate or foreign commerce or communication”
- Essentially, any computer connected to the internet

Criminal offenses

- Unauthorized access to information on a protected computer
- Leveraging unauthorized access to commit fraud for something of value worth >$5000
- Causing damage or loss to a protected computer
- Threatening to cause damage to or steal information from a protected computer without authorization

Covers worms, viruses, DDoS, computer trespass, computer fraud, computer espionage, password theft, etc.

Notable CFAA Prosecutions

Robert Morris for releasing the Morris worm

US v. Collins: against members of Anonymous for DDoSing Paypal

Albert Gonzalez for the TJX hack

Numerous cybercriminals, such as Severa

How Does the CFAA Impact Cybersecurity Researchers?

Infamous CFAA Prosecutions

US v Lori Drew: Drew created a fake MySpace account and used it to harass a young girl, who later committed suicide

- Drew was charged under CFAA for violation MySpace's Terms of Service
- ToS said fake accounts were unauthorized

Infamous CFAA Prosecutions

US v Lori Drew: Drew created a fake MySpace account and used it to harass a young girl, who later committed suicide

- Drew was charged under CFAA for violation MySpace's Terms of Service
- ToS said fake accounts were unauthorized

US v Nosal: Nosal stole a database from his former employer using credentials borrowed from a current employee

- Account sharing violated the computer use policy for the corporate network

Aaron Swartz

Developer and internet activist

- Co-developer of RSS and Markdown
- Founder of Demand Progress

Aaron Swartz

Developer and internet activist

- Co-developer of RSS and Markdown
- Founder of Demand Progress

January 2011: Aaron was arrested for crawling papers from JSTOR

- JSTOR is a for-profit publisher of academic papers
- Aaron believed research results should be available to the public
- Broke into a wiring closet at MIT and setup a laptop to download papers

Aaron Swartz

Developer and internet activist

- Co-developer of RSS and Markdown
- Founder of Demand Progress

January 2011: Aaron was arrested for crawling papers from JSTOR

- JSTOR is a for-profit publisher of academic papers
- Aaron believed research results should be available to the public
- Broke into a wiring closet at MIT and setup a laptop to download papers

U.S. Attorney for Massachusetts Carmen Ortiz charged Aaron with 13 counts under the CFAA

- Even though MIT and JSTOR decline to press charges
- 35 years in prison and $1m max fine

Aaron Swartz

Developer and internet activist

- Co-developer of RSS and Markdown
- Founder of Demand Progress

January 2011: Aaron was arrested for crawling papers from JSTOR

- JSTOR is a for-profit publisher of academic papers
- Aaron believed research results should be available to the public
- Broke into a wiring closet at MIT and setup a laptop to download papers

U.S. Attorney for Massachusetts Carmen Ortiz charged Aaron with 13 counts under the CFAA

- Even though MIT and JSTOR decline to press charges
- 35 years in prison and $1m max fine

Aaron committed suicide

The Problem of Authorization

Definition of “authorized” in the CFAA is ambiguous

- Who decides *what* computers may be accessed or are “protected”?
- Who decides *how* a computer may be accessed?

The Problem of Authorization

Definition of “authorized” in the CFAA is ambiguous

- Who decides *what* computers may be accessed or are “protected”?
- Who decides *how* a computer may be accessed?

Different circuit courts have different interpretations

- Authorization is defined by policy
  - Terms of Service, Computer Use Policy, etc.
- Authorization is defined by mechanism
  - Access control systems
  - Firewalls
  - IP blockades

Access Versus Use

Access Versus Use

CFAA criminalizes access violations

But, CFAA threats have been brought for violating use policies

Example: LinkedIn vs. HiQ

- HiQ scrapes data from LinkedIn and uses it for analytics
- The data comes from public profiles
  - Anyone may access this data, even without a LinkedIn account
- LinkedIn's ToS says you may visit the website, but you may not record anything from the website
  - How you *intend to use* the data matters

Are use violations also CFAA violations?

Cautionary Tale

Kevin Finisterre identified several serious problems with DJI drones

- Found SSL private keys and AES firmware encryption keys in DJI's public GitHub
- Gained access to DJI servers containing customer data and business records

Cautionary Tale

Kevin Finisterre identified several serious problems with DJI drones

- Found SSL private keys and AES firmware encryption keys in DJI's public GitHub
- Gained access to DJI servers containing customer data and business records

DJI had a bug bounty program

- Kevin disclosed his findings to DJI, did not go public
- DJI agreed to $30k reward

Cautionary Tale

Kevin Finisterre identified several serious problems with DJI drones

- Found SSL private keys and AES firmware encryption keys in DJI's public GitHub
- Gained access to DJI servers containing customer data and business records

DJI had a bug bounty program

- Kevin disclosed his findings to DJI, did not go public
- DJI agreed to $30k reward

However, DJI demanded an extremely restrictive NDA before paying the bounty

- Threatened CFAA prosecution of Kevin did not comply

Cautionary Tale

Kevin Finisterre identified several serious problems with DJI drones

- Found SSL private keys and AES firmware encryption keys in DJI's public GitHub
- Gained access to DJI servers containing customer data and business records

DJI had a bug bounty program

- Kevin disclosed his findings to DJI, did not go public
- DJI agreed to $30k reward

However, DJI demanded an extremely restrictive NDA before paying the bounty

- Threatened CFAA prosecution of Kevin did not comply

Ultimately, gave up the bounty and went public

Happy Ending?

DJI completely overhauled their bug bounty terms

Now one of the best in the industry

“By participating in this program and abiding by these terms, DJI grants you limited “authorized access” to its systems under the Computer Fraud and Abuse Act in accordance with the terms of the program and will waive any claims under the Digital Millennium Copyright Act (DCMA) and other relevant laws.”

-- https://security.dji.com/policy?lang=en_US

Digital Millennium Copyright Act of 1998

Intended to criminalize circumvention of Digital Rights Management (DRM) software

- Mechanisms used to prevent copyright infringement
- Copy protection on videogames, software, digital media, etc.

Criminalizes circumvention of access controls

- Regardless of whether you actually infringe copyrights

Criminalizes the distribution of circumvention tools

- Regardless of whether you actually infringe copyrights

The Librarian of Congress may issue exemptions

- Exemptions reviewed and changed every three years

Scope of the Law

What are copyright access control mechanisms?

- Encryption on copyrighted works
  - CSS → DVD, AACS → Bluray, Apple FairPlay → eBooks and music
  - High-bandwidth Digital Content Protection (HDCP) encrypts HDMI connections
- Copy protection software and mechanisms
  - SecuROM and SafeDisc for videogames
  - Mandatory USB dongles
- Watermarks
  - Steganographic marker embedded in media or software

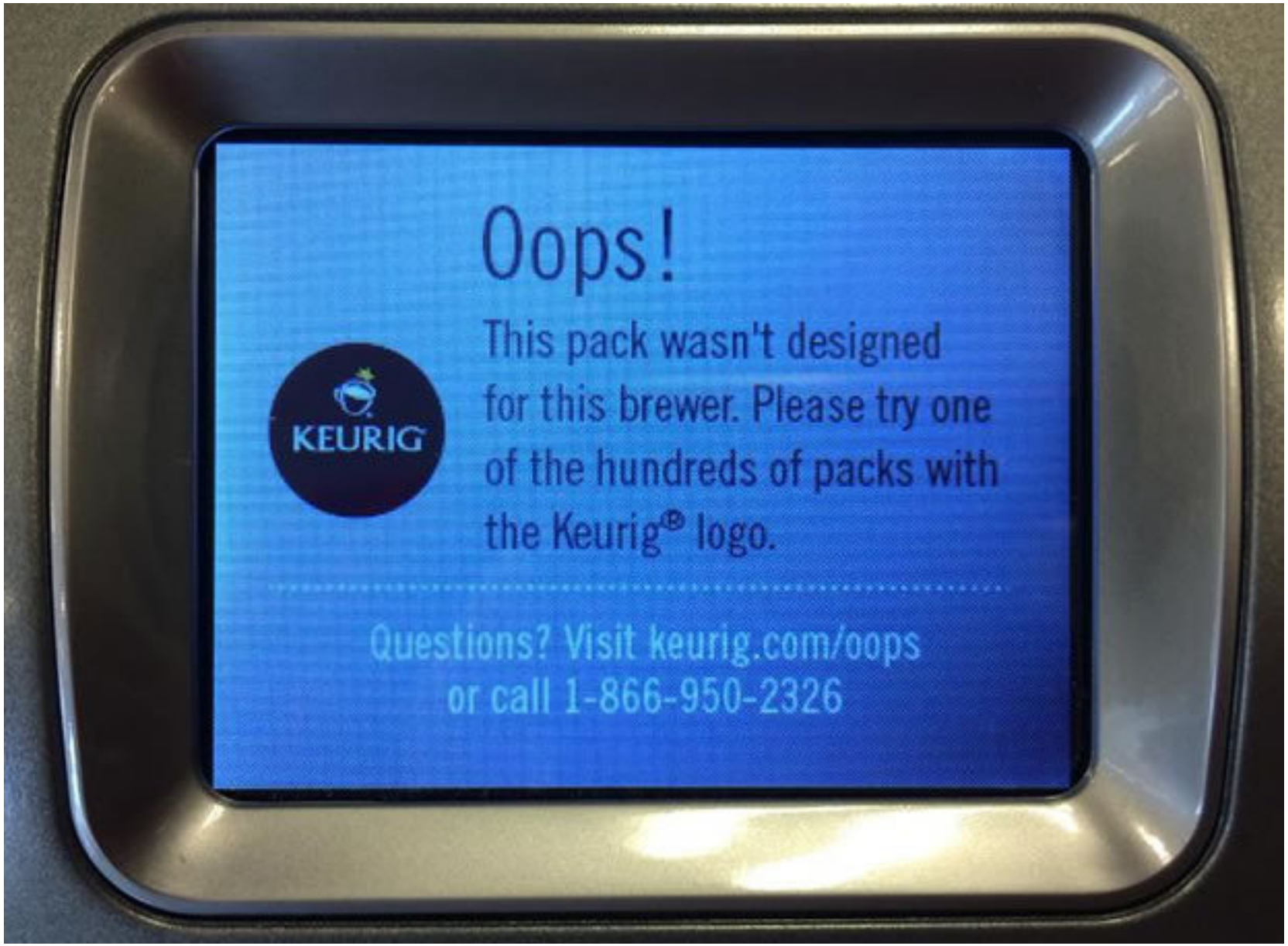
Scope of the Law

What are copyright access control mechanisms?

- Encryption on copyrighted works
  - CSS → DVD, AACS → Bluray, Apple FairPlay → eBooks and music
  - High-bandwidth Digital Content Protection (HDCP) encrypts HDMI connections
- Copy protection software and mechanisms
  - SecuROM and SafeDisc for videogames
  - Mandatory USB dongles
- Watermarks
  - Steganographic marker embedded in media or software

Unfortunately, scope of the DMCA is very broad

- Any software can be copyrighted
- Any encryption may be considered an access control mechanism
- Authentication is also an access control mechanism


Oops!
This pack wasn't designed for this brewer. Please try one of the hundreds of packs with the Keurig® logo.
KEURIG
Questions? Visit keurig.com/oops
or call 1-866-950-2326

Chilling DRM Research

2000: SDMI issues a challenge to security researchers

- Secure Digital Music Initiative
- Asked researchers to crack a digital music watermarking scheme

Team from Princeton led by Ed Felten completes the challenge

- SDMI threatens the team with DMCA claims to prevent publication

Team eventually publishes after suing SDMI

Similar fights have happened between Intel and researchers who found flaws in HDCP

Chilling Vulnerability Research

2002: proof-of-concept exploits for bugs in HP Unix

- HP threatens researchers with DMCA violations

2003: vulnerabilities in Blackboard's electronic ID cards

- Blackboard uses DMCA to halt presentation of security research

2003: vulnerabilities in GameSpy's online services

- GameSpy's lawyers threaten the researcher under DMCA
- Researcher removes findings from the web

Getting Out of Hand

Sony sues George Hotz (geohot) for jailbreaking the Playstation 3

- Required exploiting the PS3's secure (encrypted) bootloader
- Sony claimed the jailbreak allowed people to play pirated games

Getting Out of Hand

Sony sues George Hotz (geohot) for jailbreaking the Playstation 3

- Required exploiting the PS3's secure (encrypted) bootloader
- Sony claimed the jailbreak allowed people to play pirated games

Craigslist sues companies that interface with their website

- Provide tools for automating and managing posts
- Circumvented CAPTCHA to enable this functionality

Getting Out of Hand

Sony sues George Hotz (geohot) for jailbreaking the Playstation 3

- Required exploiting the PS3's secure (encrypted) bootloader
- Sony claimed the jailbreak allowed people to play pirated games

Craigslist sues companies that interface with their website

- Provide tools for automating and managing posts
- Circumvented CAPTCHA to enable this functionality

iPhones locked to the App Store and specific mobile carriers

Getting Out of Hand

Sony sues George Hotz (geohot) for jailbreaking the Playstation 3

- Required exploiting the PS3's secure (encrypted) bootloader
- Sony claimed the jailbreak allowed people to play pirated games

Craigslist sues companies that interface with their website

- Provide tools for automating and managing posts
- Circumvented CAPTCHA to enable this functionality

iPhones locked to the App Store and specific mobile carriers

Lexmark sues companies that sell aftermarket ink cartridges

- Cartridges include authentication chips

Getting Out of Hand

Sony sues George Hotz (geohot) for jailbreaking the Playstation 3

- Required exploiting the PS3's secure (encrypted) bootloader
- Sony claimed the jailbreak allowed people to play pirated games

Craigslist sues companies that interface with their website

- Provide tools for automating and managing posts
- Circumvented CAPTCHA to enable this functionality

iPhones locked to the App Store and specific mobile carriers

Lexmark sues companies that sell aftermarket ink cartridges

- Cartridges include authentication chips

Company sues former contractor for connecting to VPN

- Argues that authorization to connect was withdrawn, therefor connecting was circumvention

Notable Exemptions

Current exemptions ratified by Library of Congress in 2018

Exemptions for good-faith research on:

- Consumer electronics and IoT devices
- Medical devices
- Voting machines
  - Repped by Andrea Matwyshyn, NEU Law Professor
- Jailbreaking and unlocking phones and digital assistants (e.g. Amazon Echo)

Notable Exemptions

Current exemptions ratified by Library of Congress in 2018

Exemptions for good-faith research on:

- Consumer electronics and IoT devices
- Medical devices
- Voting machines
  - Repped by Andrea Matwyshyn, NEU Law Professor
- Jailbreaking and unlocking phones and digital assistants (e.g. Amazon Echo)

Warning: exemptions are not permanent or all-inclusive

- Must have legal access to the device or software
- Cannot violate other laws, like the CFAA

Takeaways

If you are doing security research on a device you own, or software on a device in your possession

- You need to be careful of the DMCA

If you are doing security research on a remote service via the internet

- You need to be careful of the DMCA and the CFAA

Vulnerability research on companies that do not have bug bounty programs is very risky

- However, bug bounty programs do not guarantee zero risk either!

Bug Bounty Programs

Most big tech companies have them

- Google, Facebook, Amazon, Apple…

Bug bounty platforms

hackerone bugcrowd

- Manage bounty programs for hundreds of companies

Each company’s bounty program has different rules and terms

- Read them before you start your research!

CAN-SPAM Act of 2003

Controlling the Assault of Non-Solicited Pornography And Marketing Act

Main provisions:

- Email headers cannot be spoofed
- Email cannot be sent through open relays
- Email must contain a working unsubscribe option
- Email cannot be sent to a harvested email addresses
- Emails with explicit content must be prominently labeled

Criminal and civil penalties

- Federal Trade Commission enforces civil components

The Good

Legitimate marketing emails all contain opt-out links now

Many cases of civil and criminal enforcement

- Months to years of jail time
- Penalties ranging from $10k t0 $1.3m

The Bad

Often called the YOU-CAN-SPAM act

- Enshrines an opt-out system, rather than opt-in
- Superseded stricter state laws

The Bad

Often called the YOU-CAN-SPAM act

- Enshrines an opt-out system, rather than opt-in
- Superseded stricter state laws

Fails to effectively handle affiliate programs

- Company claims “all the spam was sent by my affiliate partners”
- Company’s affiliate agreement prohibits spam…
- Even if the provision was never actually enforced

The Bad

Often called the YOU-CAN-SPAM act

- Enshrines an opt-out system, rather than opt-in
- Superseded stricter state laws

Fails to effectively handle affiliate programs

- Company claims “all the spam was sent by my affiliate partners”
- Company’s affiliate agreement prohibits spam…
- Even if the provision was never actually enforced

Law asked the FTC to study the creation of a Do-Not-Spam list

- FTC completely rejected this idea

The Bad

Often called the YOU-CAN-SPAM act

- Enshrines an opt-out system, rather than opt-in
- Superseded stricter state laws

Fails to effectively handle affiliate programs

- Company claims “all the spam was sent by my affiliate partners”
- Company’s affiliate agreement prohibits spam…
- Even if the provision was never actually enforced

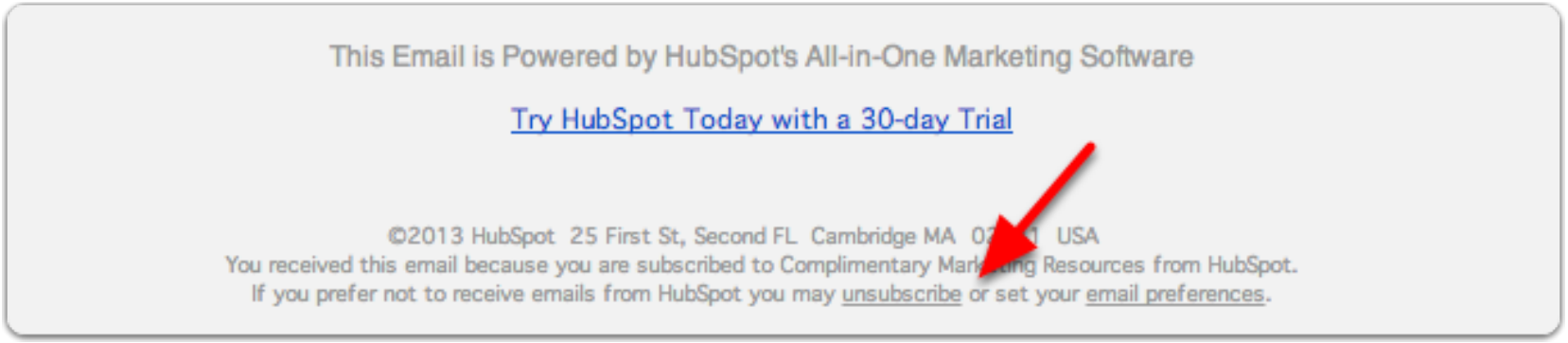
Law asked the FTC to study the creation of a Do-Not-Spam list

- FTC completely rejected this idea

Most spam is sent by criminals

- News flash: they don’t care about the law

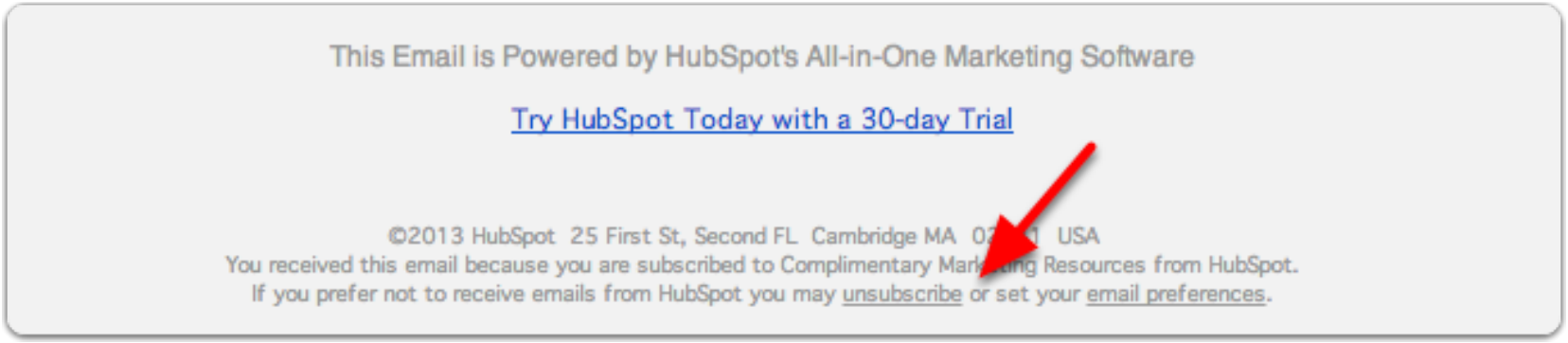
Beware The Unsubscribe Link



To be CAN-SPAM compliant, legit marketing emails all contain an unsubscribe link

Actual spam also now contain unsubscribe links. Why?

Beware The Unsubscribe Link

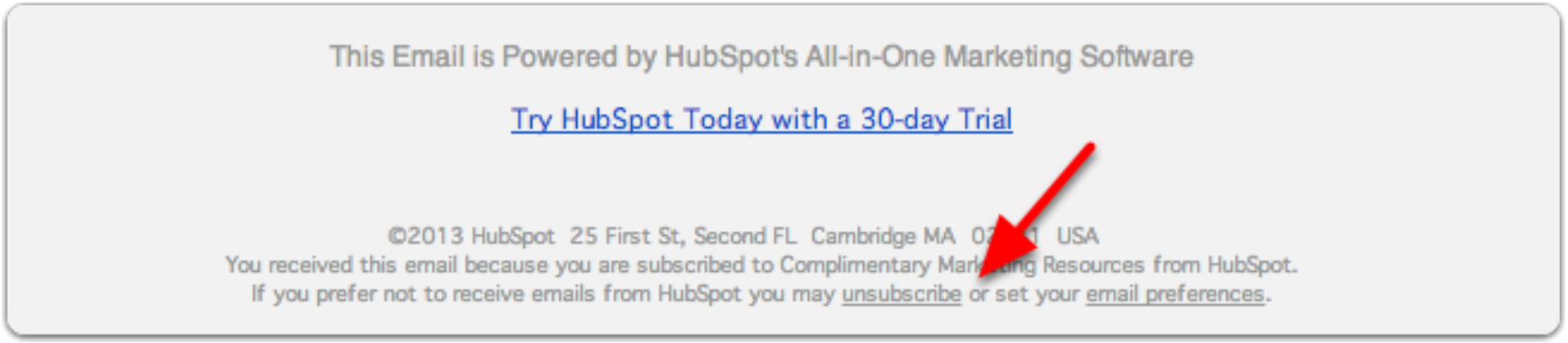


To be CAN-SPAM compliant, legit marketing emails all contain an unsubscribe link

Actual spam also now contain unsubscribe links. Why?

- The links are fake
- Lead to drive-by download or scam sites
- Clicking the link enables the spammer to determine that you saw their spam!
  - Prepare to get a lot more spam!!

Beware The Unsubscribe Link



To be CAN-SPAM compliant, legit marketing emails all contain an unsubscribe link

Actual spam also now contain unsubscribe links. Why?

- The links are fake
- Lead to drive-by download or scam sites
- Clicking the link enables the spammer to determine that you saw their spam!
  - Prepare to get a lot more spam!!

Example of unintended consequences

So Much More to Learn

Things we haven't covered:

- International law
- State law
- Intellectual property law
  - Copyright
  - Patents
  - Trade secrets
- Wiretap laws
- Privacy laws
  - US: HIPAA, COPPA, FCRA
  - Europe: GDPR (and soon, Cal Privacy in California)
  - Mandatory breach notifications

Sources

- EFF:
  - Coders' Rights Project Reverse Engineering FAQ, https://www.eff.org/issues/coders/reverse-engineering-faq
  - Coders' Rights Project Vulnerability Reporting FAQ, https://www.eff.org/issues/coders/vulnerability-reporting-faq
  - A "Grey Hat" Guide, https://www.eff.org/pages/grey-hat-guide
  - Unintended Consequences: Sixteen Years under the DMCA, https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf
- US DOJ:
  - Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and U.S. Retail Networks, https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail
  - Russian National Indicted with Multiple Offenses in Connection with Kelihos Botnet, https://www.justice.gov/opa/pr/russian-national-indicted-multiple-offenses-connection-kelihos-botnet
- Are Bug Bounty Program Safe for Whitehats?, https://www.usenix.org/node/208178
- The Confessions of Marcus Hutchins, https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/