Creating Infinite Possibilities.

SCTE
a subsidiary of CableLabs

# I Didn’t See It Coming: The Rise of the Bot


**Claire Nobles**

Project Manager 5
Comcast
Claire_Nobles@comcast.com



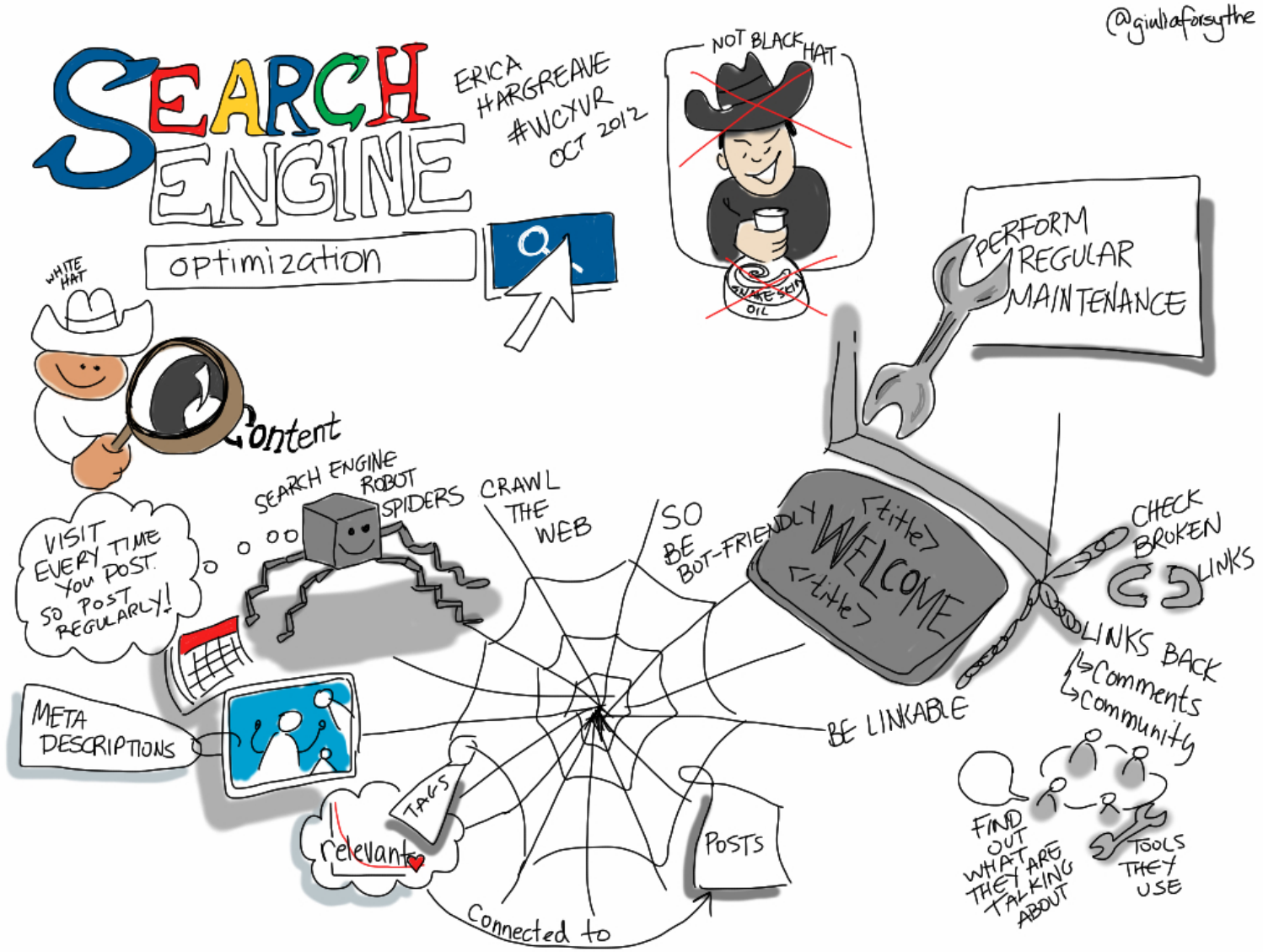
SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

# What is a Bot?

BOTNET (roBOT NETwork)

Required Bots

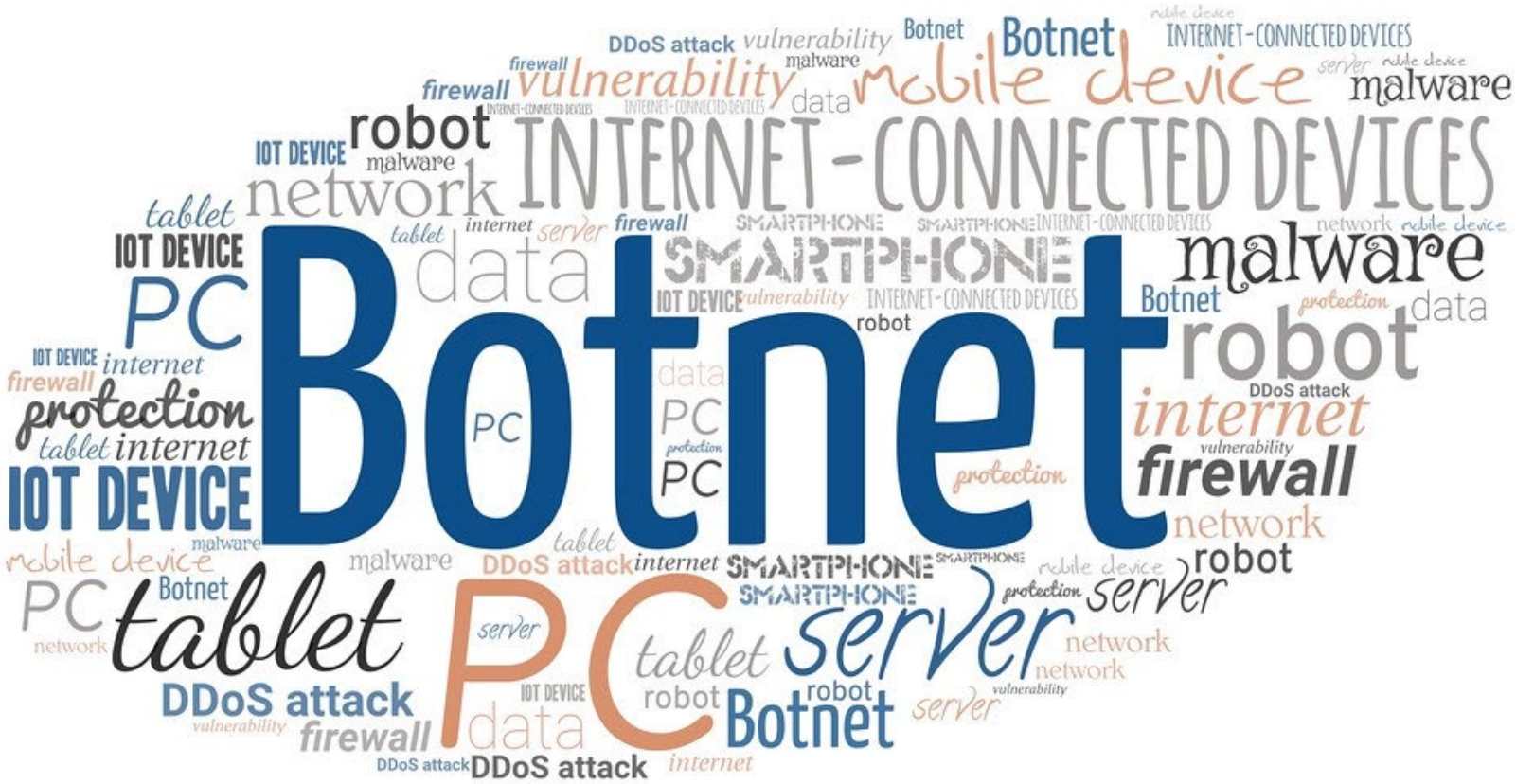


# What is a Bot?

BOTNET (roBOT NETwork)

Required Bots

Malicious Bots



# Botnet Delivery Methods





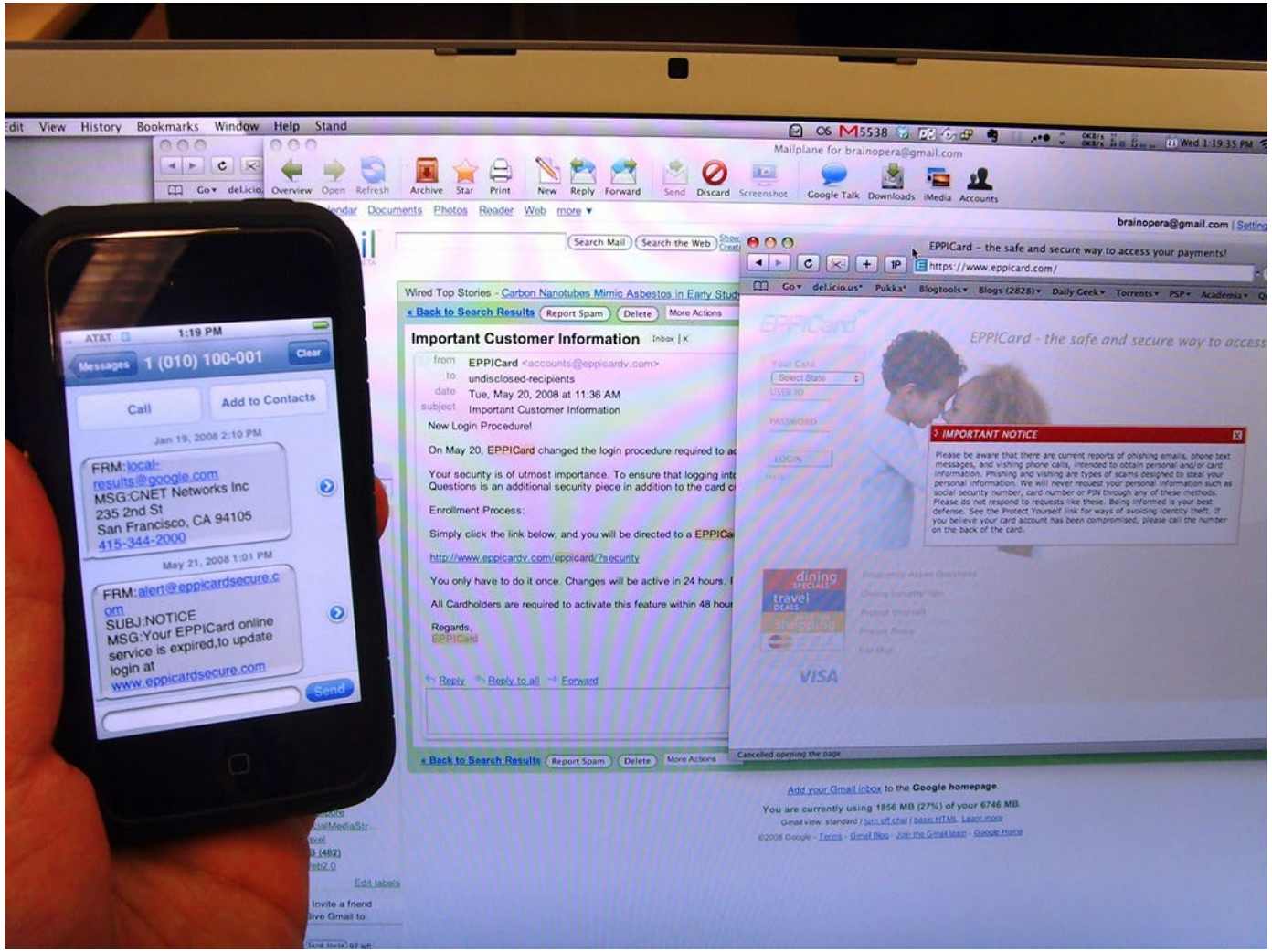
Phishing

- Appears to be legitimate source
- Act fast, limited time to think
- Malicious links or attachments (PDF, Spreadsheets, pictures etc)
- Often claims reader is compromised

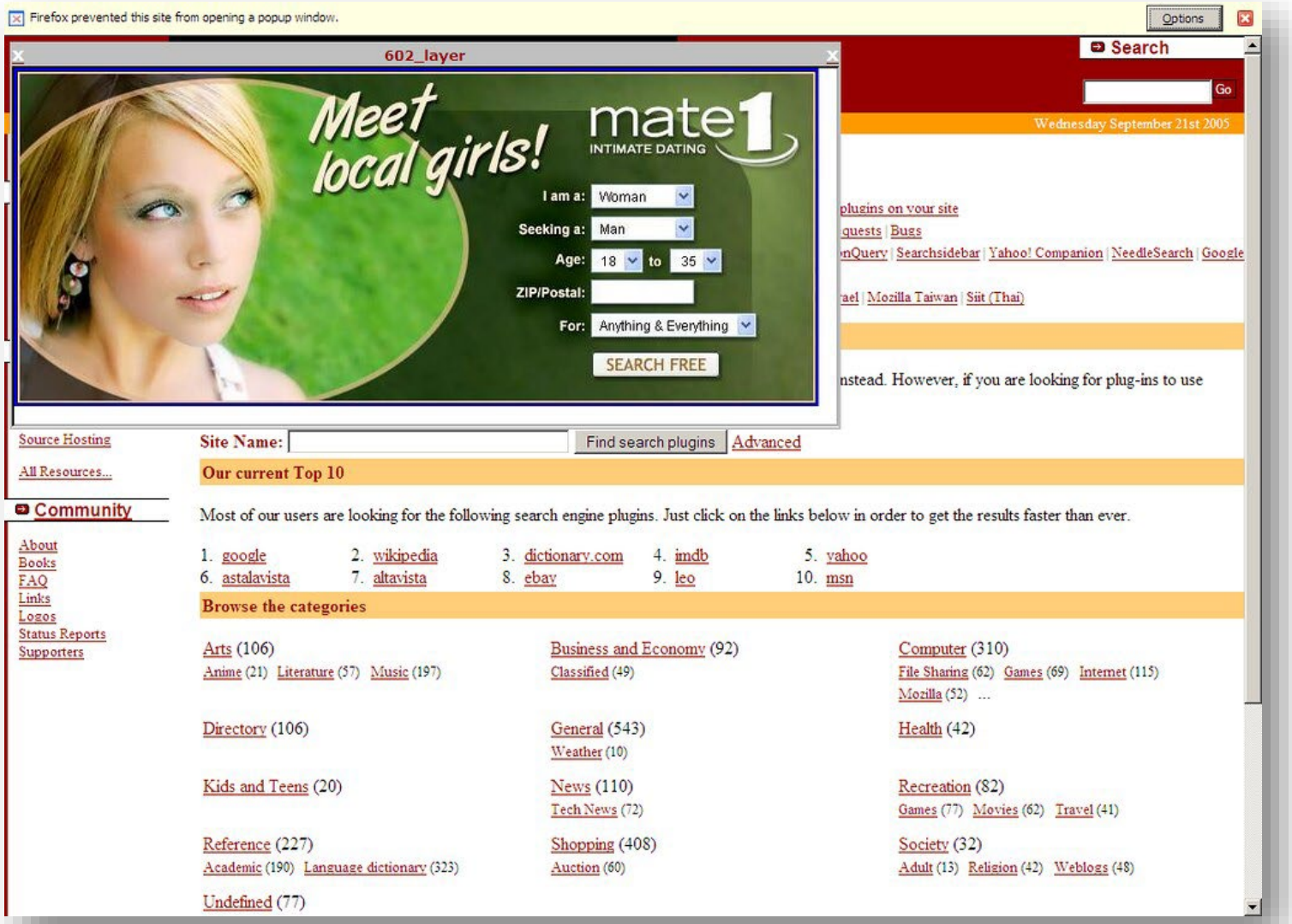
# Botnet Delivery Methods

SMShing

- URL shorteners hide destination
- Much less filtering than email
- No virus protection on most!



# Botnet Delivery Methods






## Malvertising

- Malicious pop ups/unders
- Risk increases as website reputation decreases
- Games and applications have the same risk profile

# Botnet Delivery Methods



Game and Application Cheats and cracks

- Often asks to disable AV to avoid false positives
- Sometimes embeds links to malicious content instead of payloads
- There is no reputable crack

# Payload Types



## Info Stealers

- All username and password data remembered by all browsers
- All credit card information remembered all browsers
- Can collect specific file types, including MFA tokens

"Identity Thief - Stolen Credit Card Information" by cafecredit is licensed under CC BY 2.0.

# Payload Types



Remote Access Tools

- Clients assume the victim's digital identity
- Residential IP Proxy as a Service comes with many free programs
- RESIP's charge by the gigabyte for the victim's internet and mobile data utilization

# Payload Types

## Crypto Jacking

- Covertly uses victim's computer resources (power, cooling, availability)
- Can be launched in browsers
- Can reside in high performance compute environments

# Payload Types




## Ransomware

- Deny access to files and information
- Sells or gives away all the victims encrypted data
- Includes all browser data

# Payload Types

# Email

- Misspellings, abbreviations and character substitutions
- Hyperlinks

www.rnicrosoft.com

www.paypl.com

www.amaz0n.com

### 4.1 Phishing

Phishing refers to email sent with malicious links or attachments or fake websites that attempt to appear legitimate. Using social engineering tactics to gain the readers confidence or trust, carefully worded email with malicious attachments or links to malicious or fake websites designed to defraud the victim is one of the most effective cyber-attacks that exist. Attachments such as Adobe PDF (Portable Document Format), Microsoft Excel spreadsheets and even pictures can contain distinct types of malicious payloads as categorized below. Opening any attachment effectively "executes" the code inside that attachment with the associated program. Although anti-virus programs catch some of this malicious code, often the malicious code escapes detection through code obfuscation or encryption. More often, a phishing email contains a link to a malicious or cloned website.

Since most email uses Hypertext Markup Language (HTML), hyperlinks, or links to websites, which allows the text to contain the underlying link to a website. For example, the text that reads "http://GoodGuyWebsite.xyz/" appears to point to GoodGuyWebsite.xyz. However, hovering the mouse

http://badguywebsite.xyz/
Ctrl+Click to follow link

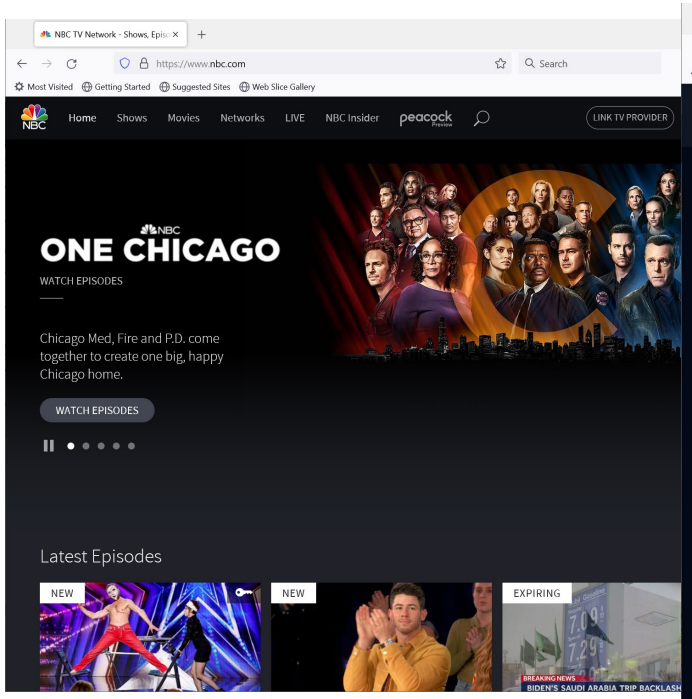




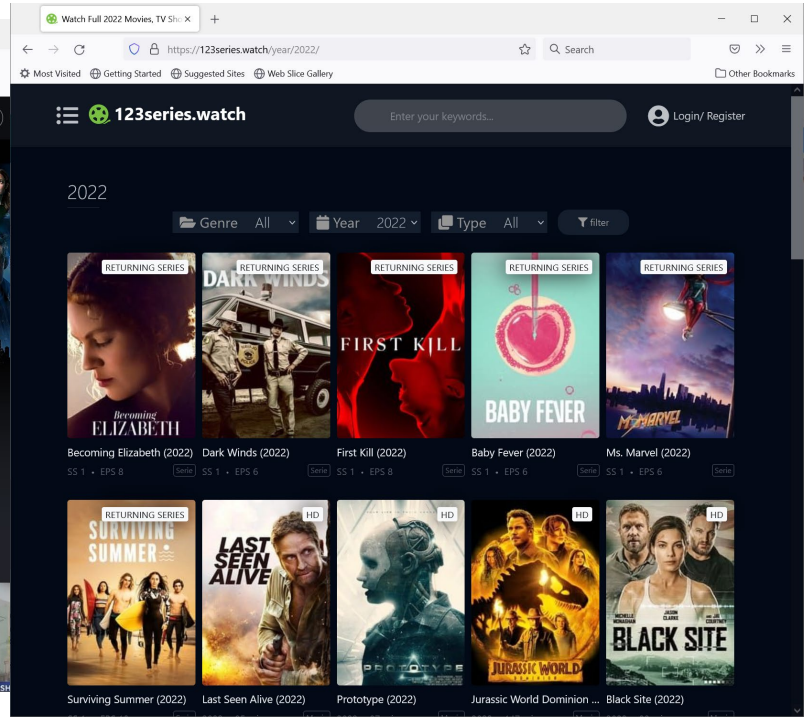
Picture from https://123series.watch/year/2022/

# Web Browsing

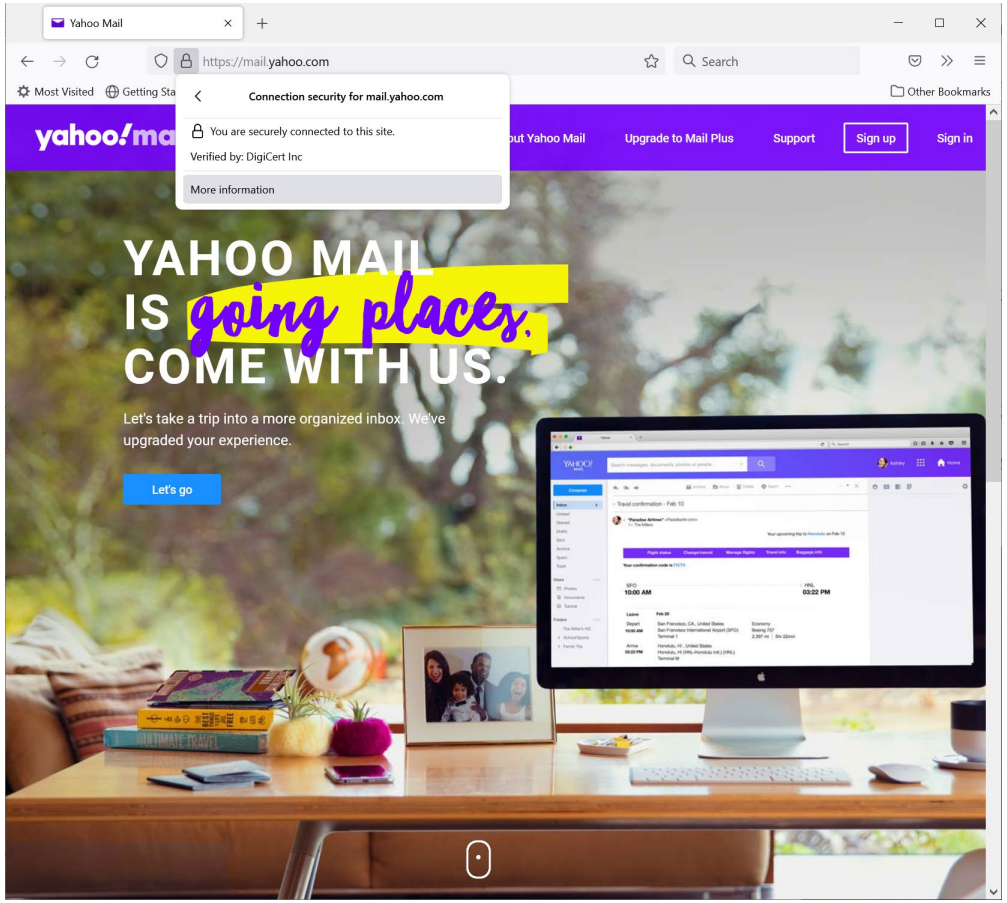
- Inverse relationship between reputation and risk
- Verify lock in navigation bar before entering any sensitive information




Picture from https://www.nbc.com



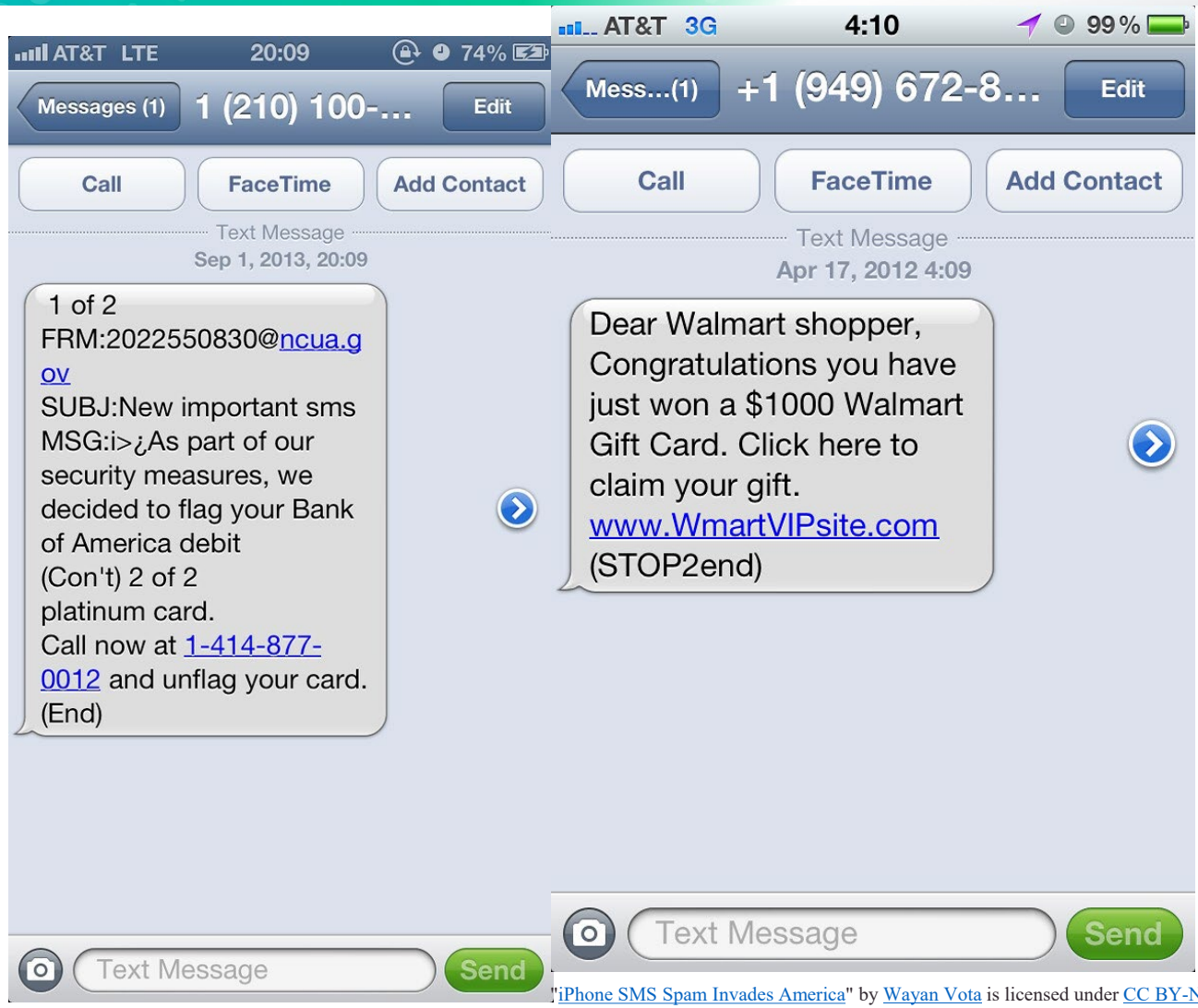

Picture from https://123series.watch/year/2022/




Picture from https://mail.yahoo.com

# SMS

- Unrecognized senders, unrecognized phone numbers or links
- Limited time offer, promises rewards for clicking/calling, exclusive etc



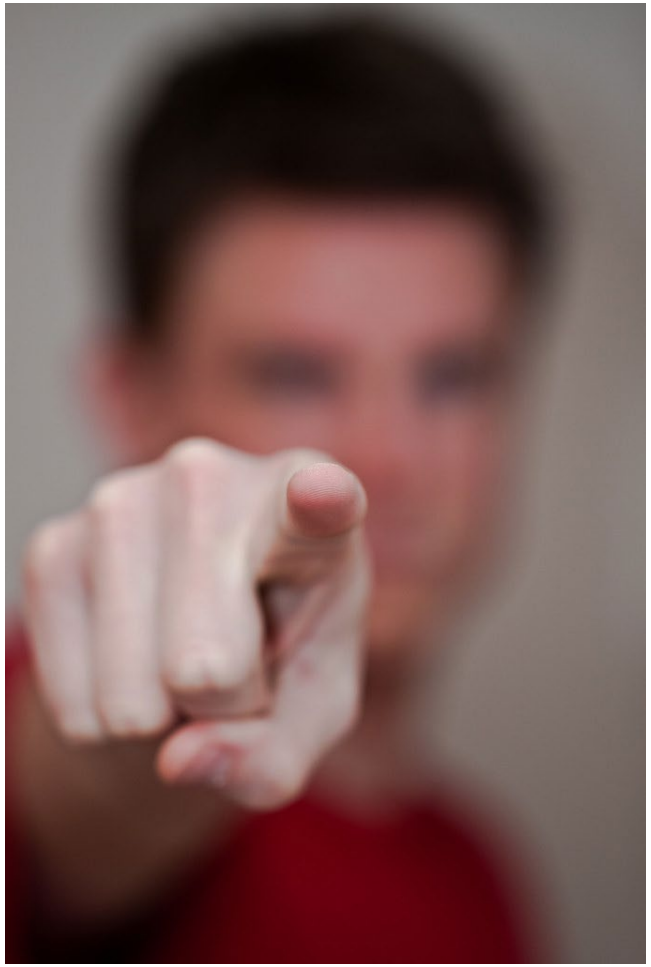

"iPhone SMS Spam Invades America" by Wayan Vota is licensed under CC BY-NC-SA 2.0.

"SMS Text Message Phishing Spam Scan" by Wayan Vota is licensed under CC BY-NC-SA 2.0.

Picture from https://mail.yahoo.com

Picture from https://123series.watch/year/2022/

# General Takeaways





- Changing passwords on an infected machine leads to re-compromise
- Storing passwords or credit card information in browsers is dangerous
- If it's free, YOU are the product
- Game & App Cracks/Cheats nearly always pack malicious payloads
- Mobile antivirus protection is just as important as a PC and is only 1 layer
- You are the next layer! Staying objective and diligent in a digital world is everyone's responsibility

# Authors



## Claire Nobles

Project Manager 5

Comcast

Claire_Nobles@comcast.com

## Andrew Frederick

Principal Engineer

Comcast

Andrew_Frederick@comcast.com

## Don Jones

Director

Comcast

Don_Jones@comcast.com

Creating Infinite Possibilities.

# Thank You!

**Claire Nobles**

Project Manager 5
Comcast
Claire_Nobles@comcast.com