Prepared Testimony of

Dr. B. Clifford Neuman

Director, USC Center for Computer Systems Security

Associate Professor of Computer Science Practice

Information Sciences Institute

Viterbi School of Engineering

University of Southern California

Los Angeles, CA

1 April 2021

Prof. Clifford Neuman is Director of the USC Center for Computer Systems Security, a Scientist with USC's Information Sciences Institute, and faculty member in the Computer Science Department where he oversees USC's computer security curricula. Dr. Neuman received an S.B. degree in Computer Science and Engineering from the Massachusetts Institute of Technology in June 1985. Upon completion he spent a year working for MIT's Project Athena where he was a principal designer of the Kerberos authentication system, widely used today on all major computer systems for enterprise network login. Dr. Neuman completed graduate studies in the Computer Science Department of the University of Washington, receiving an M.S. degree in 1988, and a Ph.D. in 1992.

IN 2020, Dr. Neuman was a speaker for the USC Election Cybersecurity Initiative which conducted a series of workshops in all 50 states targeting campaigns, election workers, policymakers, and concerned citizens that needed objective, factual tools, and information to keep our elections safe.

Thank you for the opportunity to speak with you today regarding cyber-security issues that are relevant to elections. In 2020 the USC Election Cybersecurity Initiative conducted a series of workshops in all 50 states targeting campaigns, election workers, and policymakers in to provide objective, factual tools, and information that would be important in keeping our elections safe.

As we discussed in our series of workshops, there are several important things to understand if we are to effectively protect our elections.

First, we need to understand the motivations and goals of our adversaries when they attempt to disrupt our elections. While it might seem like their goal is to change the outcome of the election, in many cases they may derive benefit from simply creating doubt about the election to challenge its legitimacy.

Second, we need to understand the different ways that an adversary will try to achieve their goals. While it might seem that changing the outcome of an election would involve changing the tabulation of votes in the systems that process completed ballots, one must consider alternative approaches such as preventing some voters from casting their ballots by disseminating incorrect information regarding election procedures, or by shutting down poling locations, or even by manipulating the voter rolls. Adversaries might also intercept ballots or election material disseminate to or collected from voters, or they might create fictitious voters to “stuff” the ballot box. An adversary can also affect the outcome of an election by “manipulating” the opinions of voters through highly targeted disinformation through social media and online “banner ads”, or through release of private campaign and personal information stolen from campaigns, candidates, and others.

Finally, it is important to understand the different computer systems that are involved in the election process (it is many more than you might think), how each of those systems can be attacked, the impact of a successful attack on one of those systems, and how the system can be protected. We also want to make sure that there are systemic (which in an election, probably means procedural) countermeasures in place that will allow us to detect and limit the impact of successful attacks on the system.

One of the most important security techniques to be applied to the election infrastructure is isolation. The systems that are most critical to the accurate outcome of the election should not be connected to the Internet. As already mentioned, there are many computers that are used at different stages of an election, and not all can be isolated in this manner. But, to the extent possible the systems that collect and count votes should not be accessible online. There may be legitimate reasons for other election systems, e.g. voter registration systems, to be available online, and if they are, that means you will need to isolate those auxiliary systems (e.g. voter registration) from the parts of the system that collect and tabulate ballots so that an adversary can not reach the backend (collection and tabulation) systems by exploiting weaknesses in the front end (voter registration systems).

While we heard of significant cyber-breaches to government systems in the latter part of 2020, specifically what is referred to as the Solar Winds breach, it is my belief that the reason this breach does not appear to have impacted our critical election systems is the level of isolation provided to the election systems from other Government networks, a concept that seemed to be well understood by election officials in most states.

I completely expect that we will see breaches of components of election systems in the future. I believe that voter registration systems will remain vulnerable since they often require access through the internet by voters. As such, these systems will always be vulnerable to denial-of-service attacks (attempts to overload the system to prevent others from registering just before the deadline), and these systems will also be vulnerable to stolen user credentials and other forms of identity theft. Within the voter registration systems, we can apply appropriate isolation and procedural controls (e.g. confirmation emails and postcards) mitigate and limit the impact of some of these breaches.

One of the most important procedural controls that should be present in voting systems is a “durable record of the intent of the voter.” This is often referred to as the “paper ballot”. It must be possible for the voter to review this “record” at the time they cast a vote so that they can be certain their intent was properly recorded. A record that is not seen by the voter can still be subverted by hacked equipment or software that “switches” votes. Having a durable record of intent allow us to verify the correctness of the vote tallies (possibly even by manual means as occurred in some places in the 2020 Presential election) and it is the only way for us to generate confidence in the tabulation process should questions arise after the election.

While Isolation can provide important protections for critical election systems, such systems are still vulnerable to subversion. This can occur through malicious software that is transferred to a system, intentionally or otherwise, through external media such as a thumb drive, or the attack can be carried through “supply chain subversion”, carried in software updates

as occurred with the Solar Winds breach on other government systems, or these subversions could potentially be carried in the election software itself. This has been claimed by some (without proof, and refuted) regarding certain election systems used in the 2020 Presidential election. Best practices to protect against this kind of subversion include secure software distribution (including signed integrity checks), source code review and verification of the software build environment, and appropriate vetting of the developer and the employees working on such systems. These steps will usually be performed as part of a certification process, such as the United States Election Assistance Commission's testing and certification program, and some state's separate certification programs.

To protect the integrity of future elections we must also consider how our computer systems integrate with all parts of the election process. For example, even votes cast manually and submitted by mail are cast using ballots printed by computer and mailed to addresses from the voter registration system, and the voter rolls are maintained on computer systems. Such ballots may have signatures verified by computer, or by election workers that view signatures on a computer screen. The danger is that through computer breaches an adversary might be able to intercept or redirect more ballots (or voters) than they could accomplish manually. Fortunately, these same systems can also improve the security of manual balloting by allowing voters to track the sending, receipt, and counting of their ballots, or by providing notices of updates to voter information. In designing the election procedures to be used in future elections it Is important to make it easier, rather than harder, for voters to cast ballots

while simultaneously making it more difficult for adversaries to cast or redirect large numbers of ballots undetected.

On March 16th the DOJ and Homeland Security confirmed their findings that they found “no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections.” However, they did find evidence of “several incidents when Russian, Chinese, and Iranian government-affiliated actors materially impacted the security of networks associated with or pertaining to US political organizations, candidates, and campaigns during 2020 federal elections.” These successful attacks on “political organizations, candidates, and campaigns” can materially impact the outcome of the elections through influence on voters.

In the same timeframe we learned of significant “successful” attacks on government and corporate systems as part of the Solar Winds breach, and Microsoft Exchange Server email breaches, which have been blamed on Russian and Chinese hacking groups. These kinds of attacks could have easily spread to election infrastructure, and you can be certain that our enemies seeking to compromise that infrastructure will keep trying.

Additional references may be found at:

https://www.electionsecurity.usc.edu/resources/

See also attached slide deck from March 25th 2021, Cybersecurity Presentation, Eastern Regional Workshop (including PA), USC Election Cybersecurity Initiative.

USC Annenberg
School for Communication and Journalism

USC University of Southern California

Election Cybersecurity Initiative

Cybersecurity and Cyber Safety

Dr. Clifford Neuman
Director, USC Center for Computer Systems Security
Scientist, USC Information Sciences Institute
Associate Professor of
Computer Science Practice
USC Viterbi School of Engineering

March 25, 2021 | Regional Workshop: DE, MD, NJ, NY, and PA

Election Cybersecurity Initiative

USC Annenberg
School for Communication and Journalism

USC University of Southern California

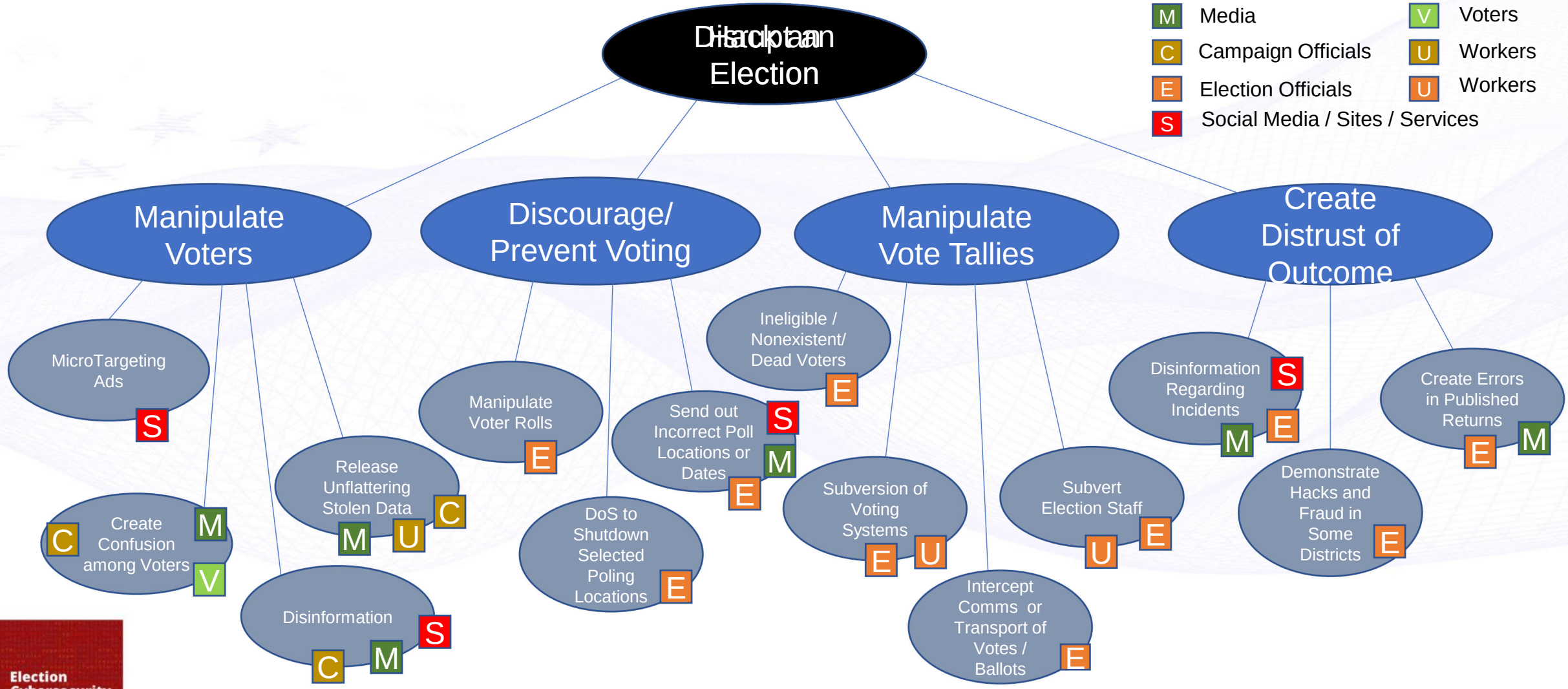
Who's Responsible for Protecting Our Elections?

We are all responsible, but some users have greater impact in defending some kinds of attacks. We will discuss the best defenses throughout the day.

USC Annenberg School for Communication and Journalism

Roadmap

USC University of Southern California



Election Cybersecurity Initiative

Source: Clifford Neuman

USC Annenberg School for Communication and Journalism

USC University of Southern California

What Happened in 2020?

- On March 16th the DOJ and Homeland Security confirmed their findings that they found “no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections.”

- However, they did find evidence of “several incidents when Russian, Chinese, and Iranian government-affiliated actors materially impacted the security of networks associated with or pertaining to US political organizations, candidates, and campaigns during 2020 federal elections.”

USC Annenberg School for Communication and Journalism

USC University of Southern California

Why is Cyber Security Important?

- In the same timeframe we learned of significant “successful” attacks on government and corporate systems: the Solar Winds breach, and Microsoft Exchange Server email breaches, which have been blamed on Russian and Chinese hacking groups.
  - These kinds of attacks could have easily spread to election infrastructure, and you can be certain that our those seeking to compromise that infrastructure will keep trying.
  - I believe Solar Winds did not affect our election infrastructure due to the level of isolation afforded to the systems used to count ballots.
  - Such isolation is an important computer security technique.

- The successful attacks on “political organizations, candidates, and campaigns” can materially impact the outcome of the elections through influence on voters.

Common Attack Vectors

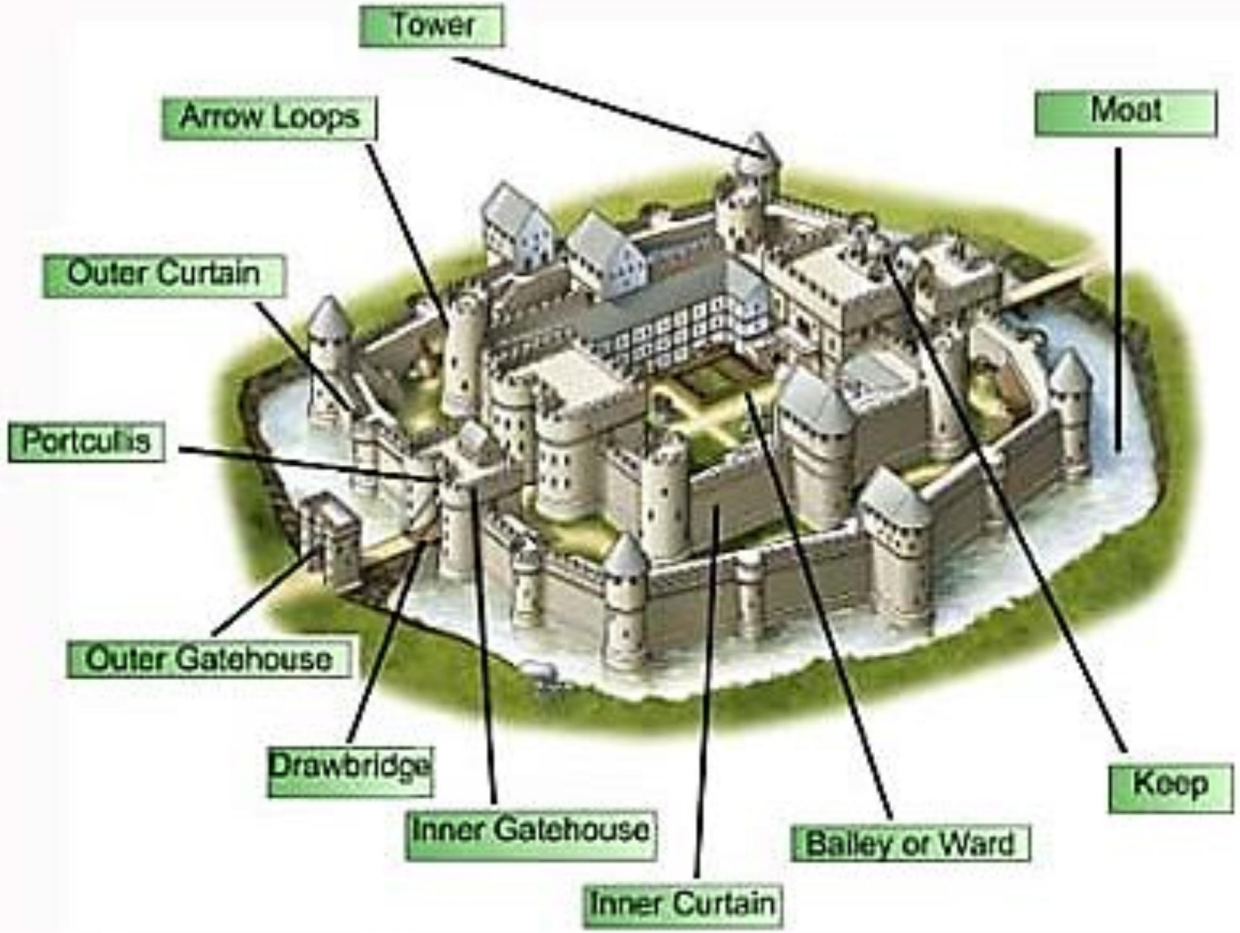
- Poor Password Management
- Malicious Code (e.g. Viruses)
- Social Engineering
- Unprotected Data
- Disinformation / Misinformation

USC Annenberg
School for Communication and Journalism

What Can We Do

USC University of Southern California

Defense in Depth

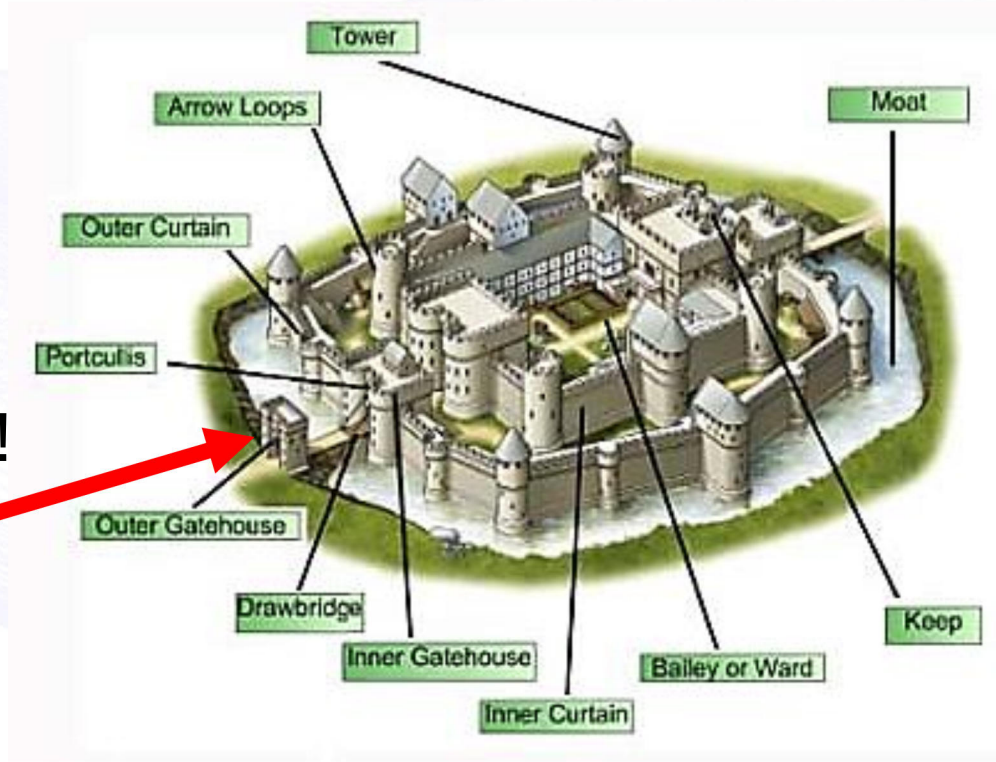


USC Annenberg School for Communication and Journalism

USC University of Southern California

Use Strong Password

- Think of passwords as the first gatehouse in the castle
- Use Passphrases as an easy way to create easy to remember passwords
  - **KeepTh3m0utOfRsystems!**
- Do not reuse passwords between accounts!
- Do not use simple passwords!
- **Do not use the password above.**

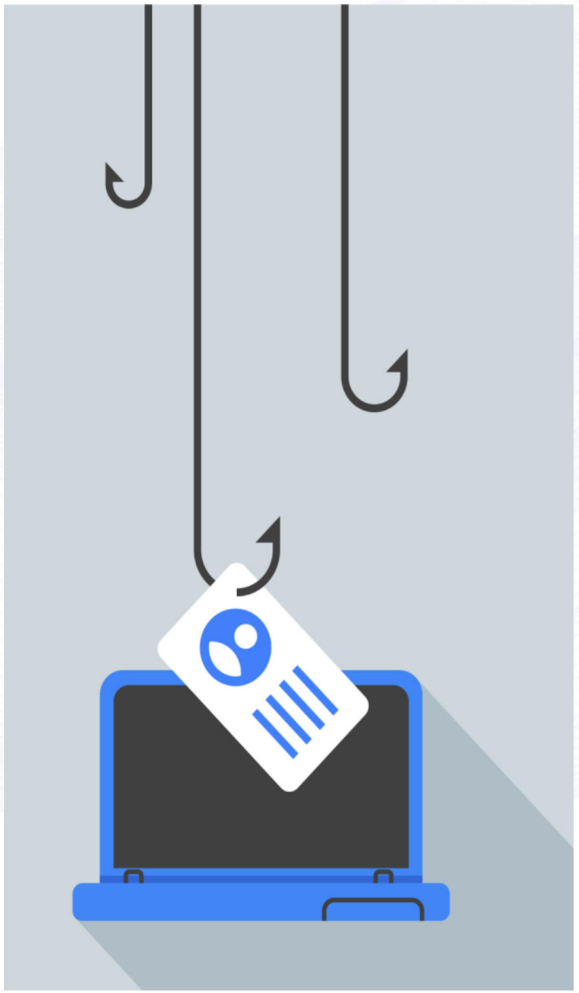


USC Annenberg School for Communication and Journalism

USC University of Southern California

Phishing

- Phishing is a method of gathering personal information (e.g. passwords) using deceptive e-mails, websites, apps, text messages, etc.
- Once your click on a link or provide a password, the hacker accesses your account or infects your machine



USC Annenberg School for Communication and Journalism

USC University of Southern California

Is Phishing effective?

- EVERYONE is a target, including you!
- #1 way hackers gain access to systems

45%

The **most believable** phishing sites trick almost half of the users.

20%

Hackers move fast: ⅕ of the accounts are accessed within 30 minutes after being phished.

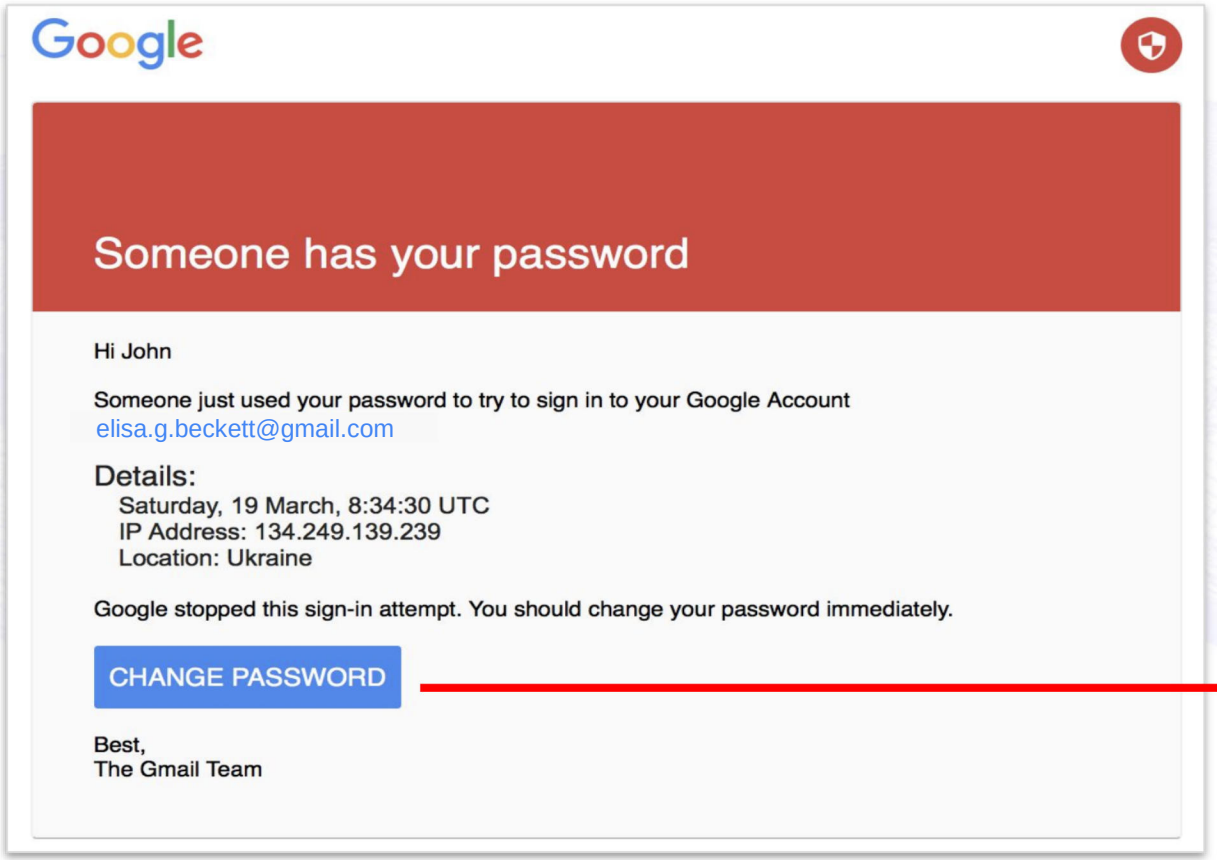
THINK/CALL BEFORE YOU CLICK

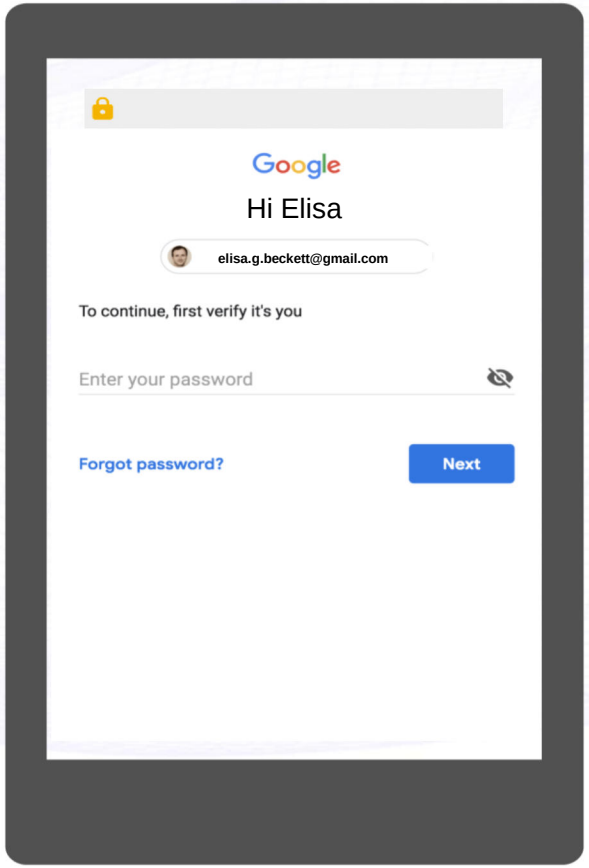
Election Cybersecurity Initiative

USC Annenberg
School for Communication and Journalism

USC University of Southern California

Phishing / Social Engineering

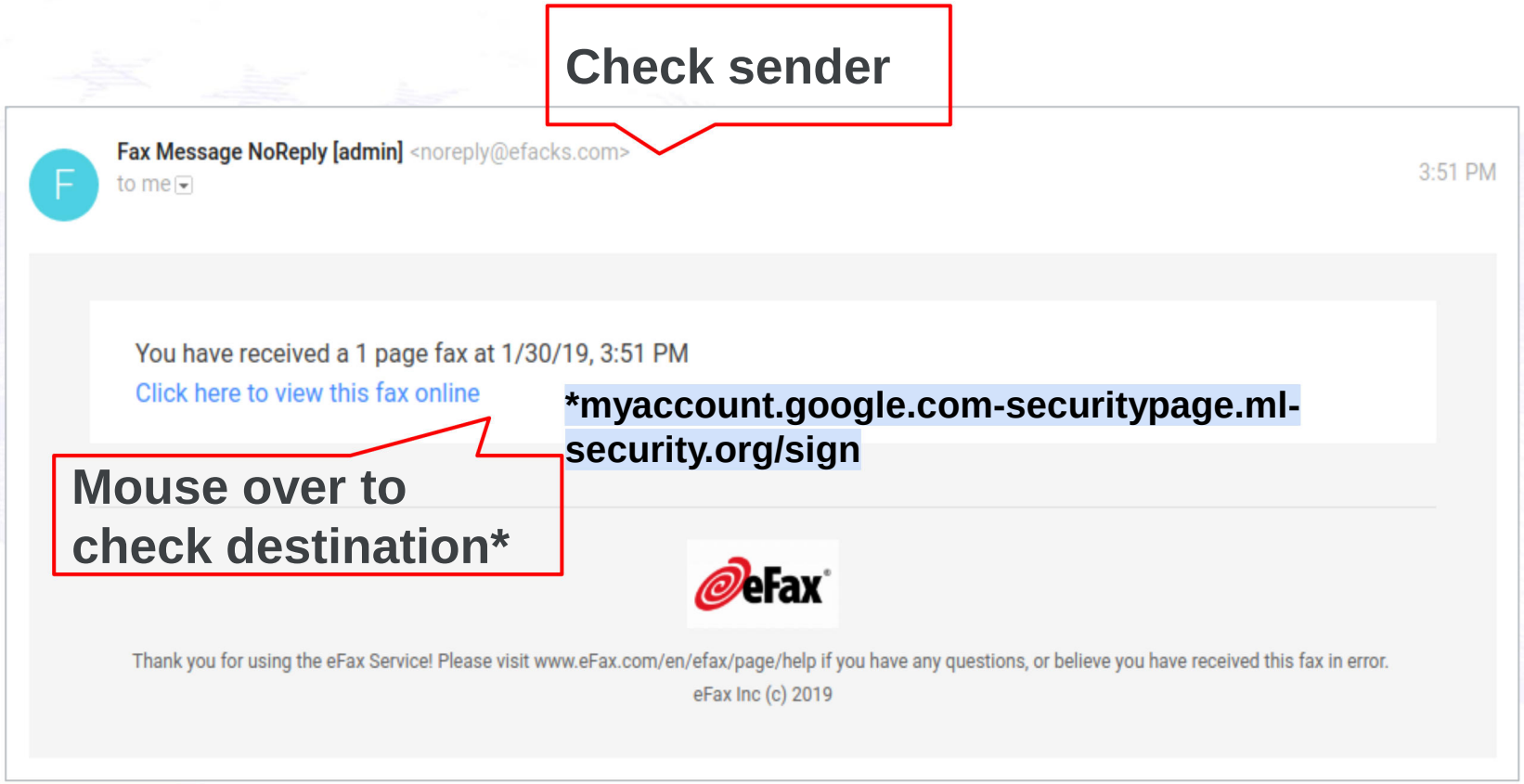




USC Annenberg School for Communication and Journalism

USC University of Southern California

Phishing / Social Engineering



Fraudulent email
Hackers will often send emails that look legit, so it's important to check the sender and the destination of any embedded links.

USC Annenberg
School for Communication and Journalism

USC University of Southern California

Phishing Quiz

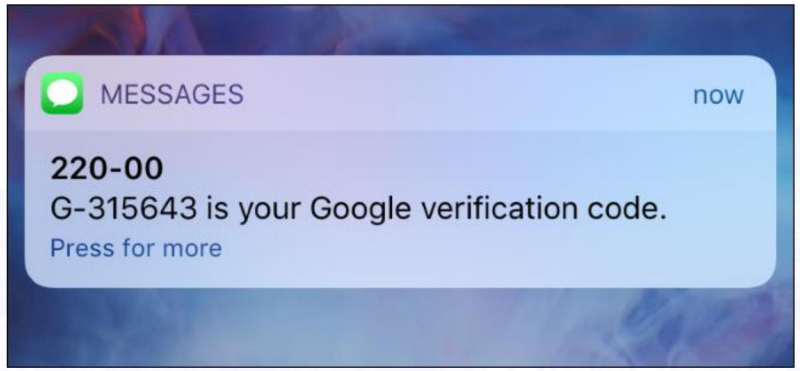
g.co/phishingquiz

Election Cybersecurity Initiative

USC Annenberg School for Communication and Journalism

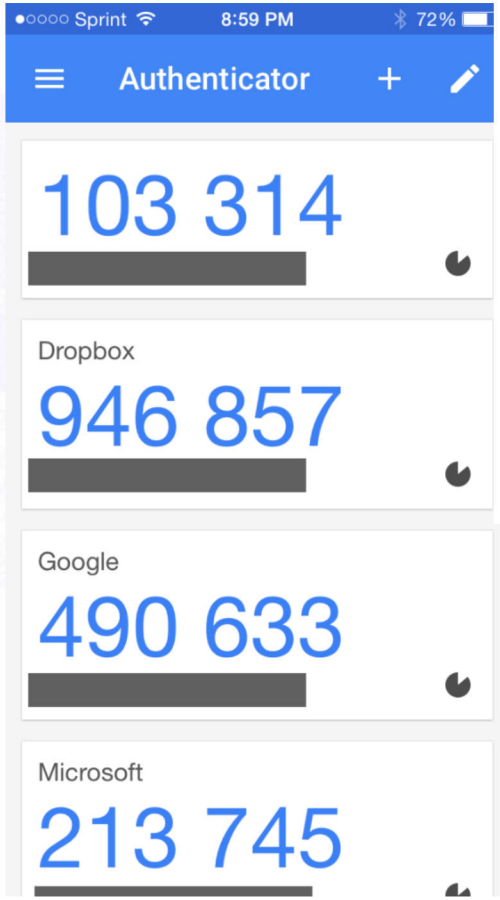
Two-Factor or Multi-Factor Authentication

USC University of Southern California



Better than passwords alone, but text messages can still be intercepted, or your phone account taken over.

- Add PIN/Passcode to your cellphone account (supported by major carriers including ATT, Verizon, Sprint).
- This helps prevent motivated individuals from moving your cell phone number to their phone to intercept texts used by second factors



Election Cybersecurity Initiative

USC Annenberg
School for Communication and Journalism

USC University of Southern California

Malware and Ransomware

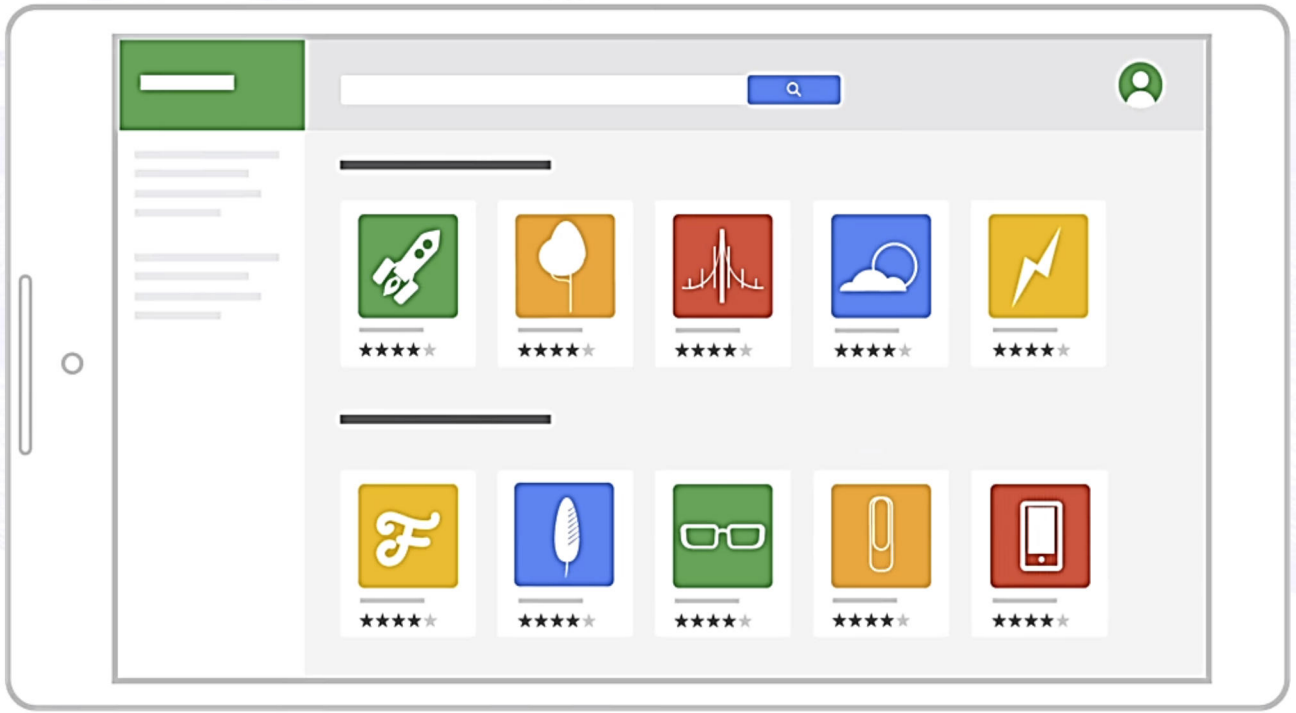
- Ransomware is when the contents of your system is locked and held for ransom
  - Or threaten to leak the data
- Typically “installed” on computers because:
  - Someone clicked on a bad link (phishing)
  - Did not patch their computers/servers
  - Downloaded “Free” software
  - Plugged in “Free” USB Drives
- Always keep a disconnected backup of your data

USC Annenberg School for Communication and Journalism

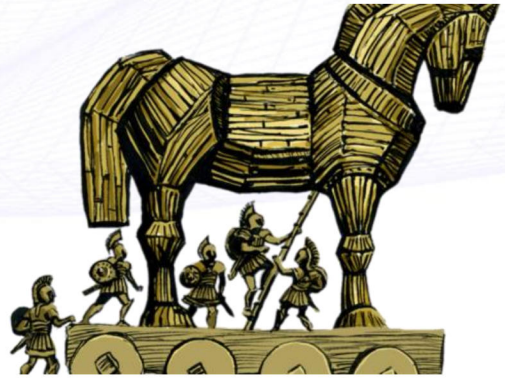
Downloads

USC University of Southern California

Always download apps only from **trusted sources**



- ✓ Install ONLY the apps you really need.
- ✓ Each new app is potential risk.



USC Annenberg School for Communication and Journalism

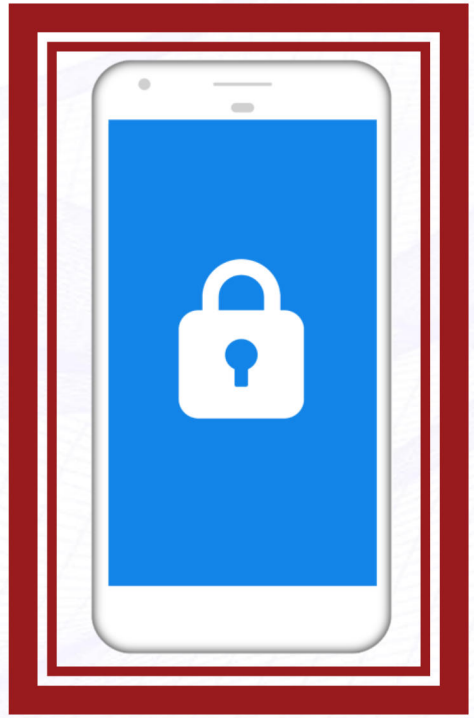
USC University of Southern California

Tips to Protect Your Communications, Data, and Systems

- When working from home (or on the road)
  - Use your organizations VPN
  - Don’t use same systems for “entertainment”
  - Be conscious of where you store sensitive data
  - Use your organizations IT Resources (email, desktops)

- Web Sites and e-mail, Chat, Voice, Video
  - Use SSL/TLS (https:)
  - Be vigilant about links, software and apps
  - End-to-end encryption

- Data at Rest (on your device)
  - Memory or Whole Disk Encryption (w/ Lockscreen/Passcode)



USC Annenberg
School for Communication and Journalism

USC University of Southern California

Questions & Answers