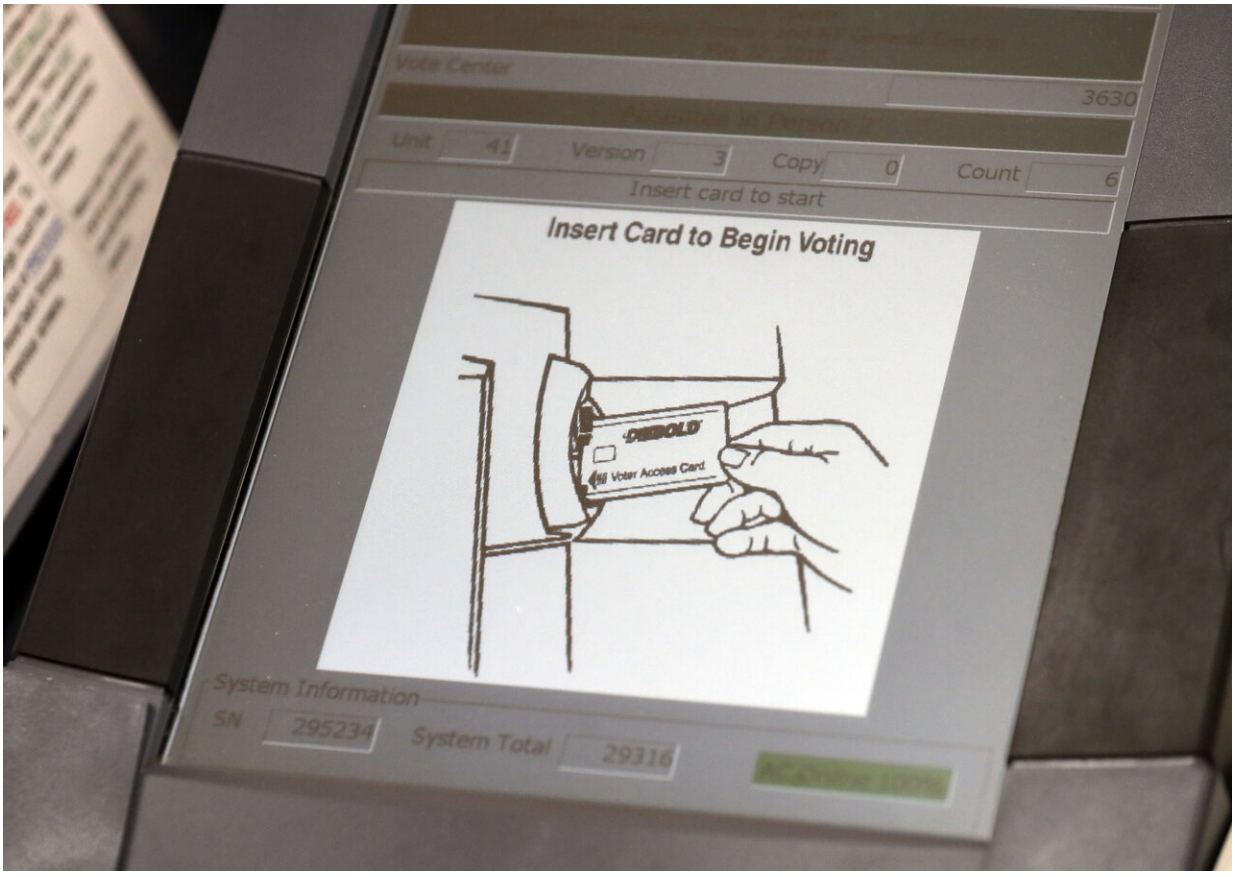
Preventing 2020 campaign cyberattacks won't be easy or cheap

May 3 2019, by Colleen Long And Christina A. Cassidy



This May 9, 2018, photo shows a touch screen of a voting machine during early voting in Sandy Springs, Ga. Whether campaigns have learned from the cyberattacks in the 2016 election is a critical question ahead of next year's presidential race. (AP Photo/John Bazemore)

While candidates were focused on campaigning in 2016, Russians were carrying out a devastating cyber operation that changed the landscape of American politics, with aftershocks continuing well into Donald Trump's presidency.

And it all started with the click of a tempting email and a typed-in password.

Whether presidential campaigns have learned from the cyberattacks is a critical question ahead as the 2020 election approaches. Preventing the attacks won't be easy or cheap.

"If you are the Pentagon or the NSA, you have the most skilled adversaries in the world trying to get in but you also have some of the most skilled people working defense," said Robby Mook, who ran Hillary Clinton's campaign in 2016. "Campaigns are facing similar adversaries, and they don't have similar resources and virtually no expertise."

Traditionally, cybersecurity has been a lower priority for candidates, especially at the early stages of a campaign. They need to raise money, hire staff, pay office rents, lobby for endorsements and travel repeatedly to early voting states.

Particularly during primary season, campaign managers face difficult spending decisions: Air a TV ad targeting a key voting demographic or invest in a more robust security system for computer networks?

"You shouldn't have to choose between getting your message out to voters and keeping the Chinese from reading your emails," said Mook, now a senior fellow with the Defending Digital Democracy Project at the Harvard Kennedy School's Belfer Center.

Mook has been helping develop a plan for a nonprofit to provide cybersecurity support and resources directly to campaigns.

The Department of Homeland Security's cyber agency is offering help, and there are signs that some Democratic campaigns are willing to take the uncomfortable step of working with an administration they are trying to unseat.

DHS has had about a dozen initial discussions with campaigns so far, officials said.

Its focus has been on establishing trust so DHS can share intelligence about possible threats and receive information from the campaigns in return, said Matt Masterson, a senior DHS cybersecurity adviser. The department also will test a campaign's or party's networks for vulnerabilities to cyberattack.

"The challenge for a campaign is they really are a pop-up," Masterson said. "They have people coming in and coming out, and they have to manage access."

It's unclear how much campaigns are spending on cybersecurity. From January to March, 12 Democratic campaigns and Trump spent at least $960,000 total on technology-related items, but that also includes technology not related to security, such as database or website services.

Former congressman John Delaney, the first Democrat to declare his candidacy for president , said he viewed cybersecurity as a fixed expense.

"It's not supercomputers cracking through your firewalls," he said. "It's really tempting emails that people respond to and give away information."

Candidates can get some advice from the Republican and Democratic national committees, which are in regular contact with Homeland Security and focus on implementing basic security protocols.

Republican National Committee press secretary Blair Ellis said the group also works with state Republican parties and emphasizes training. The organization is also developing an internal platform to share real-time threat information with state parties.

"Data security remains a top priority for the RNC," she said.

The Democratic National Committee last year hired Bob Lord, formerly head of Yahoo's information security. He has created a checklist that focuses on basics: password security, web encryption and social media privacy. This is a bigger priority than talking about the latest network protection gadget.

"What's new and interesting is fine, but it's really just about being incredibly single-minded about the basics," Lord said. "It's not glamorous, but neither is the advice for staying fit."

The 2016 attacks were low-tech, with Russian agents sending hundreds of spearfishing emails to the personal and work emails of Clinton campaign staffers and volunteers, along with people working for the Democratic Congressional Campaign Committee and the Democratic National Committee.

After an employee clicked and gave up password information, the Russians gained access to the Democratic Congressional Campaign Committee's networks and eventually exploited that to gain entry to the Democratic National Committee.

Clinton's campaign chairman, John Podesta, fell for the same trick on

his personal email account, which allowed Russians to steal thousands of messages about the inner workings of the campaign.

But it wasn't as if the Clinton campaign ignored cybersecurity. Mook said training was extensive on cyber threats, two-factor authentication was mandatory, and multiple fake emails were sent to test staffers' ability to detect phishing attempts.

The relative ease with which Russian agents penetrated computers underscores the perilous situation facing campaigns. Clinton has been talking about this with Democratic presidential candidates.

"Unless we know how to protect our election from what happened before and what could happen again ... you could lose," Clinton said in a MSNBC interview. "I don't mean it to scare everybody. But I do want every candidate to understand this remains a threat."

California Sen. Kamala Harris' campaign said it also was preaching the basics of cybersecurity with staff, such as requiring two-factor authentication and using encrypted messaging.

"All staff is being trained on threats and ways to avoid being a target," Harris spokesman Ian Sams said.

Others running in the Democratic primary avoided discussing the topic. Some campaigns, including those for Sens. Kirsten Gillibrand and Bernie Sanders, would not comment. The campaigns of Pete Buttigieg, Sen. Amy Klobuchar and Beto O'Rourke didn't respond to requests for comment.

Trump's re-election campaign wouldn't talk either.

The president has often downplayed Russia's interference in 2016. And

his staff told former Homeland Security Secretary Kirstjen Nielsen not to bring up election security during her meetings with him—saying she should focus on border security, his signature issue, according to people familiar with the discussions who were not authorized to speak publicly and spoke to AP on condition of anonymity.

Administration officials insist election security is a priority.

"We're all in in protecting 2020," Chris Krebs, head of DHS' cyber efforts, told lawmakers Tuesday at a House committee hearing-. "I'd ask, each of you: Do you know if your campaign is working with us?"

© 2019 The Associated Press. All rights reserved.

Citation: Preventing 2020 campaign cyberattacks won't be easy or cheap (2019, May 3) retrieved 26 April 2024 from https://phys.org/news/2019-05-campaign-cyberattacks-wont-easy-cheap.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.