


[Facebook](#) [Twitter](#) [Google +](#)

Every Campaign And Candidate Should Expect All Personal, Financial And Sex Data To Get Hacked From Now On

The Democrats' cyber-trauma of 2016 has inspired increased awareness — and some paranoia — about digital security. But experts say it's not enough.

By MARTIN MATISHAK

 Sen. Cory Gardner is pictured. | AP Photo

"It's pretty obvious what Russia's trying to do. All of us have had plenty of warning now," Sen. Claire McCaskill (D-Mo.) told POLITICO. | Hunter Dyke/Columbia Daily Tribune via AP

Some bathrooms have signs urging people to wash their hands. But at the Democratic National Committee, [reminders](#) hanging in the men's and women's restrooms address a different kind of hygiene.

"Remember: Email is NOT a secure method of communication," the [signs](#) read, "and if you see something odd, say something."

The fliers are a visible symptom of an increased focus on cybersecurity at the DNC, more than two years after hackers linked to the Russian military looted the committee's computer networks and inflamed the party's internal divides at the worst possible time for Hillary Clinton. But the painful lessons of 2016 have yet to take hold across the campaign world — which remains the soft underbelly for cyberattacks aimed at disrupting the American political process.

Despite making some strides in cybersecurity protections since 2016, cyber experts and researchers say, many candidates and campaigns have yet to implement standard safeguards to prevent breaches of their computer networks, websites and emails.

"It just doesn't seem to be as urgent of a concern in the conversations I've had," said Ronald Bushar, government chief technology officer for FireEye, which has long tracked the Russian hacker group that U.S. intelligent agencies say targeted the Democrats and Clinton.

MOST READ



Trump fumes at the FBI, Justice Dept. and Sessions in series of tweets

Omarosa: Trump is 'mentally declined'

Conway: Trump White House requires nondisclosure agreements

Kasich: Ohio special election 'a message from the voters'

Giuliani backtracks: 'No conversation' between Trump, Comey on Flynn

Lax state ethics rules leave health agencies vulnerable to conflicts

What Charlottesville Changed

McAuliffe: 'We ought to look at' impeachment of Trump


The Donald Trump Cinematic Universe

Is This the Next Alexandria Ocasio-Cortez?

Facebook Twitter Google +

Your email...

By signing up you agree to receive POLITICO. You can unsubscribe

 [Donald Trump and Macaulay Culkin in Home Alone 2: Lost in New York.](#)

The Donald Trump Cinematic Universe

By DEREK ROBERTSON

 [A Customs and Border Patrol agent at an American airport.](#)

Traveling While Muslim: The Case of the Exploding Chocolate

By QASIM RASHID

 [Rudy Giuliani is pictured. | AP Photo](#)

Week 64: Trump's Not Afraid of Lying to Mueller. Just Telling the Truth.

By JACK SHAFER

 [Rashida Tlaib on her first day in the Michigan legislature in 2009.](#)

Rashida Tlaib Is the Left's Way Forward

By DEREK ROBERTSON

Over the past two years, Bushar has consulted with numerous campaigns, political committees and Capitol Hill staffers on cybersecurity issues and advocated for greater investments in email security and defenses such as 24-hour website intrusion monitoring. But he said, “I don’t see a ton of that happening.”

Meanwhile, a former FBI official told POLITICO that hackers are continuing to target campaigns in an attempt to undermine November’s midterm elections. At least two senators have recently discussed a spate of cyberattacks targeting Congress.

But lawmakers and the country’s top intelligence and law enforcement agencies haven’t offered campaigns the same coordinated cybersecurity assistance they’re providing to state governments, which are receiving \$380 million to safeguard their voting machines, voter databases and other election systems.

Even with that federal help, states are largely unprepared to improve their security before this November’s elections and are off to a slow start to gird for 2020, a [POLITICO survey](#) found last month. The situation may be even more dire for political campaigns — short-lived, often shoestring operations.

When the Trump administration paraded out some of its highest-ranking officials on Aug. 2 to reinforce the government’s commitment to secure elections, Director of National Intelligence Dan Coats made it clear politicians are under attack, too. “We ... know the Russians try to hack into and steal information from candidates and government officials alike,” he said.

In recent weeks, Democratic Sens. Claire McCaskill of Missouri and Jeanne Shaheen of New Hampshire both said email attacks have targeted their Senate offices. McCaskill, a critic of both Trump and Russia, is up for reelection this year in a deep-red state and has blamed Moscow for the cyberattacks on her staff.

“It’s pretty obvious what Russia’s trying to do. All of us have had plenty of warning now,” McCaskill told POLITICO last week. “I don’t think my office and my campaign are the only ones that are taking extraordinary efforts to try to protect our information.”



ELECTIONS

Despite Trump’s assurances, states struggle with 2020 election

By ERIC GELLER

The former FBI official with knowledge of cyberattacks on campaigns told POLITICO that the assaults are ongoing and “campaigns are being targeted.” The former official said it was unclear where these efforts originated but that they are specifically targeting the midterms and “in support of continuing to undermine the democratic process.”

Essentially, the former official said, the new attacks on campaigns are similar to those that targeted the DNC and Clinton's staff in 2016: remote-access attempts to penetrate emails.

In interviews, lawmakers and campaigns insisted they have made the right security investments and have raised awareness on digital threats enough to stop hackers and foreign adversaries. Neither the DNC nor the Republican National Committee would specify the steps they have taken, citing security concerns.

Still, both parties have publicly disclosed some of their actions, such as hosting security workshops with tech companies like Microsoft. The DNC opened an "I Will Run" marketplace that directed potential campaigns to use secure communication apps made by Signal and Wickr. Some campaigns are also taking advantage of enhanced security features that Google is offering for free to high-profile targets.

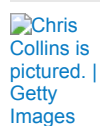
"The bottom line is that campaigns are both smarter about cybersecurity than they were two years ago, take it more seriously, and, on balance, have mitigated some of the cybersecurity risk that is out there," said Eric Rosenbach, co-director of the Harvard Kennedy School's Belfer Center for Science and International Affairs.

"That said, when you're starting from a very low bar, it's easy to show lots of improvement," added Rosenbach, who leads the center's Defending Digital Democracy Project, a bipartisan effort devoted to election cybersecurity.

Colorado Sen. Cory Gardner, who chairs the National Republican Senatorial Committee, said cybersecurity demands "constant vigilance" from campaigns.

"It really is a real-time, ongoing effort to make sure people have the tools they need to safeguard themselves and the process," he told POLITICO, adding that the NRSC's digital team has had "very lengthy, detailed conversations" with candidates, campaigns and vendors about online threats.

Gardner said the candidates he's talked to "absolutely" understand the risk of not protecting their sensitive data from hackers. "If they don't, they're not running a good campaign."



Rep. Chris Collins, fighting prosecution, seeks reelection bid

By KYLE CHENEY and JIMMY VIELKIND

In addition to the increased attention to security among campaigns and candidates, many people working in politics and on the midterms feel a growing sense of urgency and paranoia about the issue.

Hence the fliers in the DNC's bathrooms, which offer a raft of cybersecurity advice including the proper use of Dropbox or Google Drive and a warning against sending passport numbers by email. Elsewhere in DNC headquarters, warnings give employees tips about topics like enabling two-factor authentication — a step beyond passwords to protect accounts.

Similar cybersecurity alerts are posted in the bathrooms at the Democratic Congressional Campaign Committee, another organization Russian hackers breached in 2016.

The RNC is working to raise security awareness, too. "Every email that's external gets marked as 'external' in the subject line," a development that's taken place within the last couple of months.

according to a source at the RNC. (This can foil intruders who pose as colleagues or bosses while trying to trick people into giving up sensitive information.) In addition, committee staffers have to take an online security test that runs them through "a bunch of different scenarios" to assess their knowledge of best cyber practices.

One Democratic operative, some of whose emails were stolen and released during the 2016 DNC hacks, said she now avoids complaining about other people in work emails. "Everyone has people they don't get along with, so we don't bitch about people in email anymore," she said.

Another Democratic operative told POLITICO that many people working on campaigns now use secure messaging apps such as Wickr and Signal.

"We're getting more robust trainings on digital security, every six months," the person said. "People are more afraid, there's more people using password managers and being more cautious about these sorts of things."

Since April, Wickr has seen a three-fold increase in the number of campaigns that use it, according to CEO Joel Wallenstrom. He said more than half of Senate campaigns and over 70 political consulting teams use the platform.

The firm's political and government lead, Audra Grassia, said that "the vast majority of campaigns and political committees are 180 degrees from where they were in the 2016 cycle" when it comes to cybersecurity.

But that said, "there's no doubt" campaigns are "going to have a target on their back as long as elected officials make huge policy decisions," Grassia added.

In a statement, David Bergstein, the national press secretary of the Democratic Senatorial Campaign Committee, said the organization has "invested significantly in information security, has certified information security professionals on staff who provide training and we work with Senate campaigns to increase their cybersecurity awareness."

Rosenbach of the Belfer Center cautioned that while it's important for the tech firms to provide tips and capabilities for campaigns to improve their security, "it's much more important the campaign managers and the leaders of the organization to make cybersecurity a priority."

"As counterintuitive as it sounds, cybersecurity is a human problem, it's a leadership problem, it's not a technical problem," said Rosenbach, whose organization last year published a campaign cybersecurity [playbook](#).

Campaigns, he said, "should just assume from here on out, for the next several decades at least, that they will be targets for cyberattackers, both nation-state intelligence services and other nefarious individuals, who are trying to have some influence on the political situation in the United States."

Tim Starks and Daniel Lippman contributed to this report.

[Facebook](#) [Twitter](#) [Google +](#)
