

InvinciBull VPN Launches Secure Democracy Initiative to Combat Campaign Hacking

US-Based VPN Offers Free VPN to US Campaign Workers and Volunteers

East Palo Alto, CA – July 1, 2019 -- InvinciBull VPN (virtual private network) announced today a widespread initiative, intended to help protect political campaigns from hacking by nation states and other rogue actors intent on disrupting the democratic process, by offering free personal VPN service to political campaigns. Trustworthy VPNs work by encrypting data over public wifi, preventing cyber spies from stealing anything. The InvinciBull Secure Democracy Initiative is available to any and all local, state and national campaigns and their teams at no cost for the duration of the campaign.

“Humans power campaigns, and thousands of Americans work on them, many of whom are volunteers and likely rely on public wifi where their passwords, contact information and campaign details can be captured by hackers,” said June Bower, Head of Marketing, InvinciBull. “Public wifi is a necessary evil for teams that must be mobile. Thankfully a personal VPN can solve the problem,” she added.

90% of cybersecurity breaches are a result of human error¹

In 2016, thousands of campaign workers supported national candidates. Hillary Clinton had 4200 paid² and 89,000 unpaid³ volunteers. Donald Trump had 880 paid² workers. His volunteer count could not be verified but numbers ranged from thousands to one million. Each one used personal computers and mobile devices, exponentially increasing the risk of a breach.

According to the [Center for Strategic and International Studies](#), nation states including Russia, China and Iran are already targeting campaigns and the organizations that power them. They

¹ <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/>

² <https://nypost.com/2016/10/07/clintons-campaign-staff-is-five-times-the-size-of-trumps/>

³ <https://www.politico.com/story/2015/12/hillary-clinton-campaign-2016-numbers-217271>

PRESS RELEASE

note: “Dozens of attacks have already been reported on campaigns and party organizations across the country, disrupting websites and stealing documents and communications.”

US organizations intent on keeping campaigns safe recommend that campaigns use VPNs including the [FBI](#), through its [Protected Voices](#) project. Harvard’s Belfer Center published a [campaign playbook](#), which advises campaign workers -- paid and volunteers -- who want to use public wifi to take the necessary precautions beforehand. “When traveling, or before you set up your campaign office, avoid public wifi services as much as possible and use trusted wifi networks wherever possible,” the authors wrote, adding “Where possible, staffers should use a VPN. VPNs help protect against intruders when on public wifi.”

There is no way to control all the devices or wifi connections of campaign volunteers and staffers. These three steps will greatly reduce the threat:

1. **Educate.** Alert all volunteers that cybersecurity is a risk and awareness is critical.
2. **Advise.** Caution team members to avoid accessing sensitive campaign information when using public wifi.
3. **Protect.** Provide every member of the campaign team with access to a personal VPN for all their devices to automatically encrypt their data when using public wifi.

InvinciBull Secure Democracy Initiative

InvinciBull VPN is available to all campaigns and their teams at no cost for the length of the campaign. We believe in protecting our democracy and we want to do what we can to provide cybersecurity to local, state and national campaigns.

Contact democracy@invincibull.io for details.

About InvinciBull VPN

InvinciBull, launched in September 2018 from US-based cybersecurity pioneer Finjan, is a US-based personal VPN that lets users easily access the content they’re looking for without the risk of being hacked or tracked. Designed to be easy to use, it’s available for computers and mobile devices. It has a proprietary auto-protect setting so you’re always safe and anonymous. Unlike other VPNs, InvinciBull never collects user data, ever.

InvinciBull is a signee of the Center for Democracy & Technology [Signals of Trustworthiness](#).

PRESS RELEASE

CONTACT:

Bonnie Rothman for InvinciBull

bonnie@companyb-ny.com

914-500-5150