



Usenix Security 2021 *

“Why wouldn’t someone think of democracy as a target?”

Security practices & challenges of people involved with U.S. political campaigns



Sunny Consolvo
Google

Patrick Gage Kelley
Google

Tara Matthews
Google

Kurt Thomas
Google

Lee Dunn
Google

Elie Bursztein
Google

August 2021



Security, Privacy, and Anti-Abuse Research

How John Podesta's email got hacked, and how to not let it happen to you



Oct. 2016

Google

How the Russians hacked the DNC and passed its emails to WikiLeaks



July 2018

Macron Leaks: The anatomy of a hack



May 2017



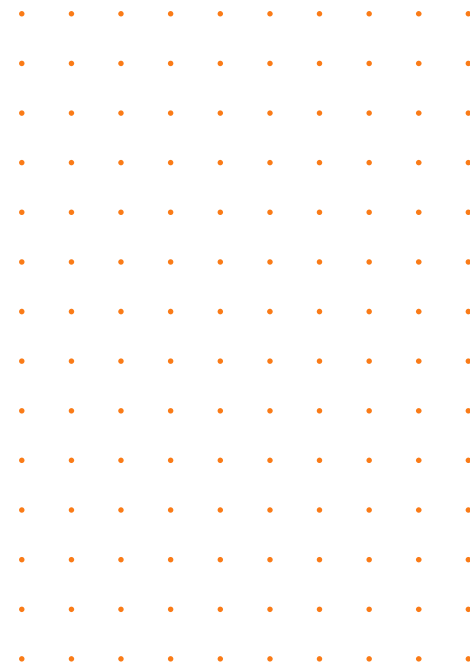
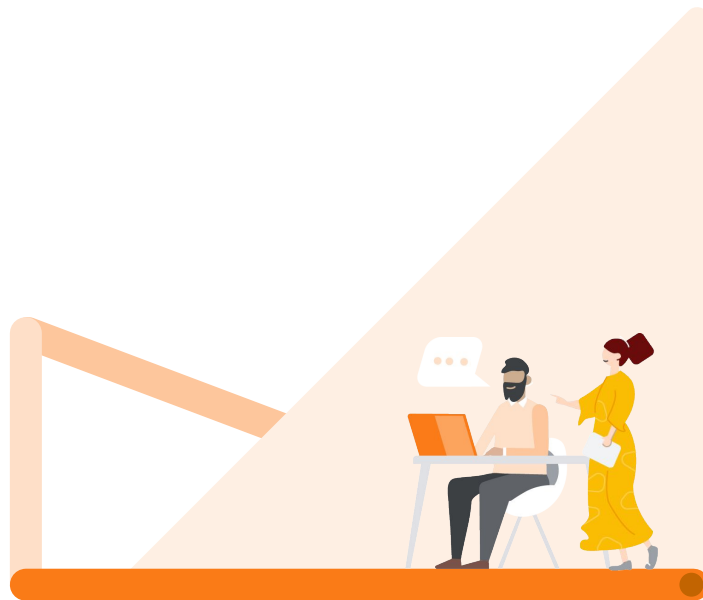
Security, Privacy, and Anti-Abuse Research



Security and politics should be separate...
If you're a candidate, **you should win or lose on your best day**, based on who you are. **Not because your email got popped** and posted online by a [nation-state cybersecurity team].”

- A study participant [emphasis added]

Research



Qualitative research

28 people involved with political campaigns in the U.S.

Roles

- candidates
- campaign managers
- digital directors
- research, strategy
- security / IT staff

Organizations

- political campaigns
- party committees (nat'l, state)
- super PACs
- campaign-specific service / support providers
- academia

2 main security factors

Work culture

Tech practices and vulnerabilities



[Campaigns are] **totally transient**,
and almost everybody gets hired in
the 3 months prior to the election...

There's really very **few incentives for
any kind of [security] rigor.**

Because you're up against the clock, and
faced with the ticking clock, everything pales."

— **A study participant** [emphasis added]


Different culture




They are
short-lived

They are
chaotically busy

They are
resourced constrained



They have
amorphous boundaries



Account use

MANY accounts are used for campaign work



- workplace system(s)
- communication tools(s)
- social media
- video / phone conferencing
- personal communications accounts
- and so on...

Some accounts are
**hyper-shared or
hyper-owned**

Not just campaign accounts


Accounts **not used for campaign-related work** are also targeted

Anything that can derail, embarrass, or otherwise disrupt could be a target




Some important aspects

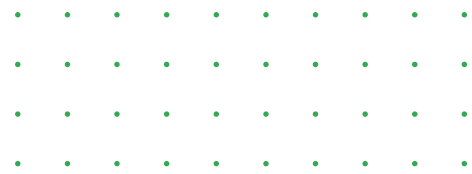
It's **unusual for campaigns to have IT staff**



Only the individual
can access all
accounts

This means they need to...

- understand that there's a real risk
 - do something about it
 - know what to do about it
 - prioritize doing something about it
- 

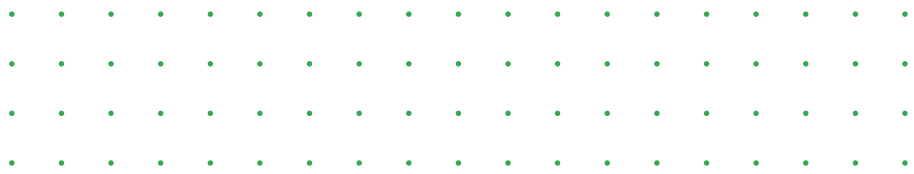


[What are nation-states after?]

“Emails, communications, anything that could compromise the campaign, make it look bad...”

Anything that makes the campaign or the staff look bad...”

— A study participant [emphasis added]



2FA practices

Heard of and probably have used 2FA

2FA is under-utilized on targeted accounts

Weaker 2nd factors are often used



Common 2FA concerns

Too much **time & effort**


Fear of **account lockout**

Hyper-shared & hyper-owned accounts




Different factors

Different factors = **different levels of security**



They know 2FA is
important, BUT


...



don't know or
can't explain why

aren't aware that they should use it
to protect **most of their accounts**

Risk & outcomes



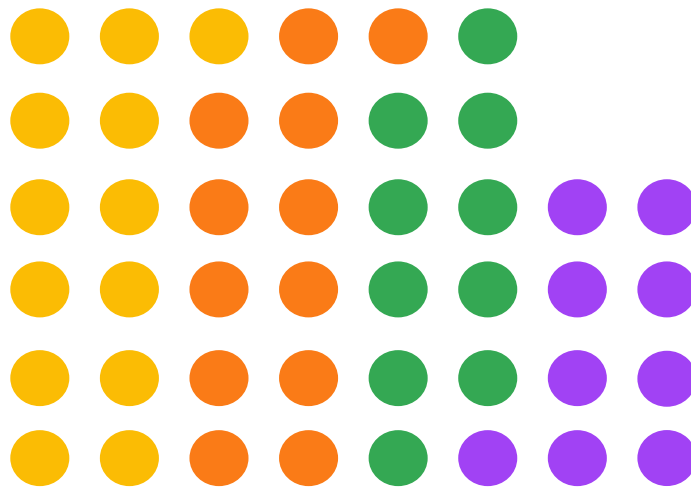
Campaigns face an **outsized risk** of being attacked

The **outcomes can be outsized** too



Expert roundtable

44 experts from 28 organizations



Expert roundtable's focus

Improve security practices on political campaigns

Single, consistent piece of
top advice for 2020

Feedback on our
research findings

Tailored advice & education

Security advice & education
that is **tailored to their
needs and context**

Prioritize!

Not everything can be critical

Exactly
what to do & why

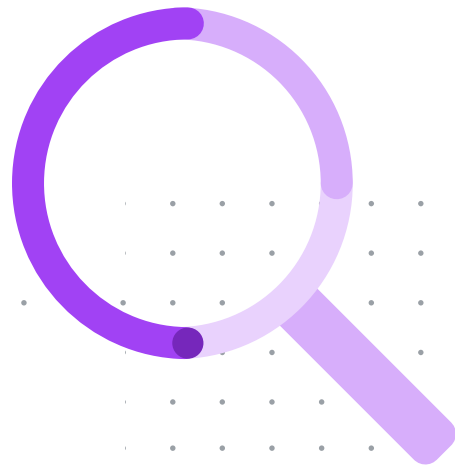
Consistent
message

More research

From deep, **foundational research**
to tactical **usability studies**

Around the world

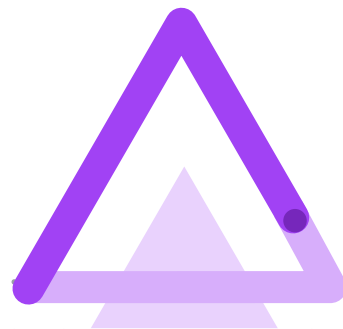
Across various **types of campaigns**
& **campaign workers**



Improved protections

Very robust, very usable
security protections

Standardization of
offerings & experience



(Perceived)
time & effort

Default settings

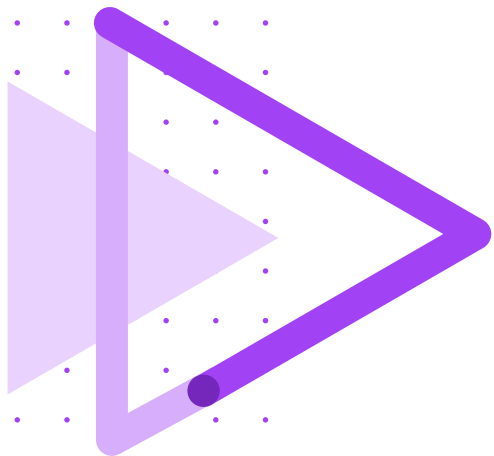


“What is 100% true... is that foreign adversaries want information... The faster we all realize that, the better off we’re going to be...

to see politics and campaigns at all levels as a fundamental piece of democracy that needs to be protected . . .

For sure foreign adversaries are trying to attack our systems... Why wouldn’t someone think of democracy as a target?”

— A study participant [emphasis added]



A big thank you



Our research participants



Our roundtable attendees



The many people at Google who helped make the research & roundtable happen