Digital Security & U.S. Political Campaigns: Expert Roundtable

September 2020

Executive summary

More than 40 leaders and experts from across the political spectrum, the technology industry, and academia came together this summer in a Google-organized virtual roundtable on improving digital security practices on political campaigns.

Our goal was to come up with a consensus piece of digital security advice to deploy during this cycle, 2020, to everyone who is working on, with, or in support of a political campaign. We hope that the promotion of a single, consistent piece of advice by relevant companies and organizations will improve understanding and adoption.

We selected advice that would provide real protection against the heightened digital security threats that this population faces, while being a reasonable ask of a population that works in a fast-paced, hectic, temporary environment where security is not the top priority. Together, the majority of roundtable attendees agreed to a top piece of advice for people involved with campaigns:[1]

> **For your most important accounts—your personal and campaign accounts for email, social media, and banking—only use the strongest form of Two-Factor Authentication (2FA) that's available, ideally hardware security keys.**

In this report, we describe our motivation for helping protect people involved with campaigns and detail the top piece of advice (strong 2FA). We then describe other pieces of advice that were highly ranked by roundtable attendees—with the intent that these would be the next pieces of advice for people who are willing to do more. We also describe a recommendation for campaign organizations, the methodology used in the roundtable, and sample text and graphics that can be used or modified to promote the top piece of advice.

---

[1] A note on ***people involved with campaigns*****:** we use this term to not just cover the paid staffers hired directly by campaigns, but also to include senior staff and advisors, the candidates, close friends and family, hired consultants and firms, volunteers, and any other campaign support provided by external organizations, national committees, state parties, etc.

Report contents

Authors

Sunny Consolvo, Patrick Gage Kelley, and Tara Matthews, Google

Contributing Authors/Organizations: In alphabetical order by first name

- Benjamin Block, DCCC (Democratic Congressional Campaign Committee)
- Elizabeth Howard, Brennan Center for Justice at NYU School of Law
- Ginny Badanes, Microsoft's Defending Democracy Program
- Jeff McCrady, NRCC (National Republican Congressional Committee)
- Jude Meche, DSCC (Democratic Senatorial Campaign Committee)
- Kamy Akhavan, USC Dornsife Center for the Political Future
- Michael Kaiser, DDC (Defending Digital Campaigns)
- Mike Sager, EMILY's List
- Rachel Holland, Facebook
- RJ Friedman, dayONE Cyber
- Saleela Khanum Salahuddin, Facebook
- Shuvo Chatterjee, Google

And representatives from the following organizations:

- America Rising Corporation
- Axiom Strategies
- CGCN
- D3P (Defending Digital Democracy Project)
- DCCC (Democratic Congressional Campaign Committee)
- DigiDems
- DNC (Democratic National Committee)
- Dropbox
- Facebook
- Google
- Harvard Kennedy School's Belfer Center for Science & International Affairs
- Higher Ground Labs
- Johns Hopkins University
- NRCC (National Republican Congressional Committee)
- NRSC (National Republican Senatorial Committee)
- Princeton University
- Rice University
- RNC (Republican National Committee)
- RNC Convention
- Slack
- TAG Strategies
- USC (University of Southern California) Dornsife Center for the Political Future
- USC (University of Southern California) Viterbi School of Engineering

Protecting people involved with campaigns

Research conducted by Google, media reports, high profile breaches, and continued attacks have highlighted weaknesses in modern political campaign infrastructure and digital information management. Many attacks on campaigns hinge on targeting individuals and their accounts, most often through social engineering attacks like phishing. Unfortunately, there are many aspects of campaign work that make phishing difficult to prevent, both at the structural level and the individual level. This includes campaign workers' use of many accounts (including personal accounts and shared campaign-related accounts); a lack of security/IT administration across those accounts; a large amount of work happening across domains, platforms, and services; a lack of cybersecurity training; and a fast-paced, hectic, temporary, environment where security is not the top priority.

Challenges. The general consensus from the roundtable was that campaign security is a hard problem. People involved with campaigns want to do the right thing, but they see cybersecurity as being difficult, not high enough priority, and maybe not worth the effort given all the other things they must do. These challenges are further complicated in the 2020 cycle by the pandemic that is drastically changing how campaigns work.

This isn't something that can be fixed by one organization. Everyone needs to make changes to improve security on campaigns, including party committees, technology companies, the government, and everyone who works on / with / in support of campaigns. Several attendees—especially security experts—emphasized that even if it is followed, a single piece of advice is not going to adequately mitigate all threats that people involved with campaigns face, and some worried that the advice could result in giving people a false sense of security, leading to riskier behaviors.

What we can do. While not unanimous, most of the attendees of our roundtable believe something can still be done to help improve the state of cybersecurity on campaigns and lay important groundwork for every campaign to establish a stronger security culture. We recognize that asking for too much change at once, or even for one thing that is not realistic, will likely lead to inaction and could encourage the dismissal of future recommendations.

With this in mind, we believe that if the top piece of advice—turning the strongest available form of 2FA on personal & campaign accounts for email, social media, and banking—is consistently shared and promoted by the roundtable attendees and other influencers in the space of politics, it has a real chance of being followed, which in turn, will improve (though not fully fix) the state of security for campaigns. And hopefully, after people follow the top piece of advice we promote, they will do more.

Top piece of advice

Security professionals have suggested copious pieces of advice for people working on political campaigns. These guides and checklists are often extensive, and though many contain great advice, they can be overwhelming to the many people who work on, with, or in support of campaigns. Our goal was to select one top piece of advice that companies, organizations, and influencers could promote, to increase the chances it would be adopted. When selecting a top piece of advice, one important criterion was how feasible it would be for campaign workers to follow, given their current understanding of and attitudes toward security. Beyond usability, we examined the added security protections and relevance to common attacks people involved with campaigns face. Using these criteria, here we summarize the benefits and limitations discussed at the roundtable (not an exhaustive list of all of the pros and cons) of the top piece of advice to promote for 2020.

Turn on the strongest form of 2FA for your most important accounts

Using Two-Factor Authentication (2FA) is the first, and most important thing someone involved in political campaigns can do. This includes *all* staff (from the most junior to the most senior), the candidate, vendors/consultants, and ideally the candidate's close family members and friends, as well as anyone with access to material that could embarrass or negatively affect the campaign.

However, what *kind* of 2FA do people involved with campaigns need to turn on, and on *what accounts* do they need to turn it on?

What second factor: hardware security keys
Different kinds of second factors provide *meaningfully* different levels of account protection. Because the threats this population faces include sophisticated, targeted attacks by well-funded and determined attackers, we believe that hardware security keys should be used wherever they are offered, and weaker second factors should be disabled. When security keys aren't an option for certain accounts, a "security prompt" or a code-generating app[2] should be used. If none of the above are available, using text codes via SMS is better than no 2FA.

What accounts: personal & campaign accounts for email, social media, and banking
We recognized that asking people involved with campaigns to set up the strongest available form of 2FA on *all* of their accounts may cause people to give up before they begin, as they may see this as too much work. We recommend that people start by turning on the strongest available form of 2FA for their personal and campaign email account(s), then their social media accounts, and then their primary banking accounts, especially if those social media or banking accounts are used for or linked to the campaign.

[2] Examples of code-generating apps include: Duo Mobile, Authenticator by Google or Microsoft, Authy, etc. This report is not meant as a recommendation or endorsement of any particular tool. Please evaluate any tools properly for your own use case before using them.

We include personal email account(s), because they have been and continue to be targeted by attackers[3], since *any* communications can be sensitive and used to harm an individual or the campaign[4], and attackers may perceive personal email accounts to be easier targets than accounts with security practices mandated by a company or organization. Campaign work often happens in personal email accounts, and attackers target email because they know that leaked communications—even from personal accounts, even if they're not about the campaign—can seriously damage the campaign.

2FA makes account hijacking more difficult. It can help limit access to sensitive data in accounts, and since email accounts can be leveraged to access other types of accounts (through password reset links sent via email), it helps to prevent that too. Securing email accounts also serve as another line of defense—they're where notifications about suspicious password reset or other account change notifications are sent for a wide variety of accounts[5].

Once the strongest form of 2FA has been turned on for email, social media, and banking accounts, it's a good idea to also turn it on for their cloud-based storage / shared doc environment, password manager, other financial accounts, and any other accounts that are important. This applies to both their campaign *and* personal accounts.

If people do the above, they will be taking a big step toward helping protect the campaign and themselves. It's also a great idea (for themselves and the campaign), if they add 2FA to their other accounts, especially if they use the same password for multiple accounts.

Pros for 2FA

- **Effectiveness.** 2FA can currently be effective at defending against phishing, the most common attack for campaigns. This is especially true when hardware security keys are enabled as the second factor with weaker backup forms disabled.
- **Usability.** With a small amount of effort and education, everyone involved with campaigns should be able to set 2FA up, and then benefit from long-term protection.

---

[3] For example: David E. Sanger & Nicole Perlroth, Russian Intelligence Hackers are Back, Microsoft Warns, Aiming at Officials of Both Parties, The New York Times, (September 10, 2020); David E. Sanger & Nicole Perlroth, Chinese Hackers Target Email Accounts of Biden Campaign Staff, Google Says, The New York Times, (Jun 4, 2020); and Nicole Perlroth & David E. Sanger, Iranian Hackers Target Trump Campaign as Threats to 2020 Mount, The New York Times, (October 4, 2019).

[4] For example: Andy Kroll, John Podesta Is Ready to Talk About Pizzagate: The former Clinton campaign chairman is among the victims still recovering from a vile conspiracy theory that ended in gunfire, Rolling Stone, (December 9, 2018); and Amanda Robb, Anatomy of a Fake News Scandal, Rolling Stone, (November 16, 2017)

[5] For these notifications to be an effective defense mechanism, the user has to see them, understand what they might mean (e.g., if they didn't initiate the action that triggered the notification, someone may be trying to break into their account), and take action. This means that email addresses and phone numbers used for account recovery (including where password reset links are sent), should be up to date and checked often, so that if someone is trying to break into an account that way, the user is likely to notice and might be able to take action before any damage is done, or at least limit it. It's a good idea to review the phone numbers and email addresses that are tied to accounts (e.g., the account's back-up/recovery contact info) to ensure they're up to date.

- **Cost.** Most providers offer weaker forms of 2FA for free. While hardware security keys—the strongest and recommended form of 2FA—do have a cost, federal campaigns can get these free through Defending Digital Campaigns (DDC).

Cons for 2FA

- **They've heard it before and haven't done it.** While most people involved with campaigns have heard of 2FA and probably use it on at least one of their accounts, they haven't fully followed previous advice for campaigns that has suggested turning it on across many or all accounts, and they likely aren't using the strongest kinds, like hardware security keys. Repeating the same old advice probably won't work, which is why this report outlines what should be highlighted when promoting the strongest forms of 2FA.
- **It's nuanced.** Most people don't understand *how* 2FA protects their accounts or that the different kinds of factors offer meaningfully different levels of security. This has been complicated by many years of messaging saying that 2FA is an important protection and that SMS codes are good enough for the general population. But now, *for this population*, 2FA SMS should be replaced with—not supplemented by—stronger factors wherever possible.
- **They might not realize that they're a target.** People also may not realize that no matter what their role is with the campaign, their risk level is different than the general population's. They really do need to use the strongest factors offered and disable weaker ones.
- **It can feel like it's not easy.** While the usability of 2FA has come a long way, it can still feel confusing, annoying, and inconvenient, particularly for people who have a million other things to do and don't want to add any extra steps to logging in to an account. They may also think they're using it on more accounts than they actually are.
- **Sometimes it's actually not easy.** There are situations where 2FA is actually difficult. For accounts regularly accessed by more than one person, for example, the campaign's *Press* account, 2FA SMS often requires the person whose phone number is registered with the account to pass around the code to whoever is trying to get in that day. If the second factor isn't available when needed, someone can end up locked out of their account. Worse, if any weaker forms are left on the account as backup options (e.g., if hardware security keys are enabled, but SMS codes aren't disabled), attackers can still break in via the weaker forms. While most providers offer some form of 2FA, those offerings are not standardized, which complicates the task of turning it on across multiple providers.
- **It's not a panacea.** Sophisticated attackers can phish numeric codes or trick someone into confirming a security prompt at just the right time, leading to our emphasis on using hardware security keys with weaker factors disabled. A truly determined, well-funded attacker might be able to bypass hardware security keys (e.g., by compromising the device itself). If the population doesn't understand this, they may end up with a false sense of security that leads to riskier behaviors. 2FA also focuses on account security, and not other threats faced by the population (e.g., malware and viruses, information campaigns).

Notes on delivering the advice

We realize that people involved with campaigns are incredibly busy, have probably heard something about 2FA before, and may not understand the different types of 2FA. To help mitigate some of those challenges, we recommend the following when promoting the 2FA advice:

- The various companies, organizations, influencers, and individuals who help to promote the advice should **consistently say that this is the first and most important action** people involved with campaigns can do to improve security for the campaign.
- **Update existing 2FA advice:** people involved with campaigns have already heard about 2FA, yet the uptake isn't where it should be. Update the advice to focus on motivating and educating them about second factors and accounts that are most relevant to the attacks *they* face.
- **Be clear about why they should do this,** including that they are part of a high risk population and what it helps to protect them from. For example, 2FA helps them to avoid being responsible for a hack that derails the campaign or having embarrassing information leaked about themselves or others.
- Be clear about the stronger protections afforded by certain second factors.
- Get **influencers** for the population to share the advice.
- Get the **candidate, campaign manager, and senior staff** to share the advice, and ideally make it a policy for the campaign.

While there are many excellent security advice guides for campaigns, some of which offer relatively short, tactical advice, we are encouraging those who read this report in advance of the 2020 election to focus on encouraging the population to turn on the *strongest available* form of 2FA on their most important accounts, as outlined above. We also don't intend to replace the other guides with a single top piece of advice. Rather, we hope that people will become more motivated to read the guides, and to do even more to protect their and the campaign's security—including the suggestions in the next section.

Other highly ranked pieces of advice

If people want to do more to protect their and the campaign's security after they turn on the strongest available form of 2FA for their most important accounts, we outline suggested follow up advice in this section, summarized in the table below. We don't think these "runners up" pieces of advice should be promoted first, but these items did rank highly in our roundtable discussions and research. Using the same criteria as above, we describe this additional advice and summarize some key benefits and limitations. We aren't presenting these in order of priority. Rather, if you're sharing this advice, we suggest prioritizing based on the specific group or community you're working with.

Advice	Pros	Cons
Turn on the strongest available form of 2FA for important accounts, starting with campaign *and* personal accounts for email, social media, and banking	• Effective against most common attacks • Relatively easy to use • Often free	• Differences in factor strength not well understood • Known advice that isn't being followed • It feels annoying or difficult
Use encrypted communications	• Fast, easy, free, and familiar • High level of protection for sensitive data • May help prevent data from being kept too long in combination with built in retention controls	• Only helps with certain types of communication • Some communications will still need to happen in other channels • May remain susceptible to insider attacks
Take security awareness training	• Highlights practical actions individuals can take • Provides some protections and awareness • Helps build a security culture over time	• Requires time, energy, and access to good, up-to-date trainings • Won't cover all attacks • People have limited attention
Turn on auto-updates for apps and devices	• Prevents inexpensive, known attacks • Easy for people to turn on • Long-term benefits	• Won't prevent against many social engineering attacks • May not provide as much benefit, as updates are often auto-enabled or already enabled
Use a password manager	• Benefits can be similar to 2FA and greater when sites don't offer strong 2FA options • Limits damage if and when passwords are breached or otherwise stolen	• Doesn't necessarily prevent social engineering attacks • Requires some user thought • Substantial set up time • Can potentially lead to account lockouts if unavailable
Build a culture of security	• Long-term safety and adaptability against many types of attacks • Does the most to raise the bar, by absorbing all of the above advice and more	• Will never be the top priority in all situations • Takes a long time to achieve, with a substantial gap from where we are today

Use encrypted communications

Using end-to-end encrypted communications is becoming more standard across campaigns due to inroads made by Signal, Wickr, and other platforms that make this easy to do. While this is a positive change, it's relatively narrow in scope given the large number of other modes of communication that continue to be used in tandem on campaigns.

Pros of encrypted communications

- Fast, free, easy, & familiar to a growing number of staff.
- More likely to mean data isn't kept as long, if content is set to expire.
- High level of security for some of the most sensitive data, for anyone willing to use the tools.

Cons of encrypted communications

- Narrow scope: doesn't help protect accounts, devices, or non-communications data.
- Hard to secure *all* communications without adherence to policies that consider the ecosystem of communications, tools, transient staff, and personal relations.
- May remain susceptible to insider threats[6].

Take security awareness training

Having people involved with campaigns **take security awareness training on how to avoid phishing and other common security attacks,** take more advanced training if they are willing, and encourage others to take training helps to establish a stronger culture of security. And once people involved with campaigns are armed with helpful knowledge to avoid and respond to common attacks—especially attacks where they may be specifically targeted, like a spear phishing attempt—the campaign will be better positioned to avoid a variety of attacks.

Pros of security awareness training

- Directly highlights the importance of individual responsibility and meaningful actions.
- Helps people avoid some security attacks, including some forms of social engineering.
- Supports building up a culture of security over time.

Cons of security awareness training

- Requires time, energy, and access to high-quality, up-to-date training materials.
- May not prevent mistakes from busy, stressed people.

---

[6] For example: Oscar J. Serrano, Misogyny, corruption and leaked messages: the story of the demise of Puerto Rico's governor, The Independent, (July 27, 2019)

Turn on auto-updates for apps & devices

One of the simplest things for people involved with campaigns to do is **turn on auto-updates for their devices' operating systems, as well as desktop and mobile apps.** This should be done, but given the number of places where it is becoming a default without user intervention, we believe it is not the *highest* priority piece of advice to encourage for the 2020 cycle.

Pros of auto-updates

- Prevents inexpensive, known, common compromise attacks.
- Easy for users to enable, leading to benefits that are automatic and long-term.

Cons of auto-updates

- Narrow security gains (new devices often already have this enabled; it doesn't help with account security or other device compromise vectors).
- Slight inconvenience of a possible new UX, install time delays, and the need to restart the device or app occasionally.

Use a password manager

Using **strong, unique passwords stored in a password manager** that is tied to the browser is another effective way to fight phishing, data breaches, and password guessing. When people use the same password for multiple accounts, they make it trivially easy for a single phishing attack or password breach to lead to their other accounts being hijacked. Additionally, **for certain attacks (e.g., on sites that don't support hardware security keys), password managers may actually be more effective than weaker forms of 2FA**. However, the upfront effort and time investment to set them up well is significant and has presented a real barrier to adoption.

Pros of using strong, unique passwords in a password manager

- It's very important to use a strong, unique password for each of a person's most important accounts. Password managers make it feasible and even easy for people to use even longer and stronger unique passwords, on *all* of their accounts, which prevents certain common, inexpensive attacks.
- Once it's properly set up, many people actually find it easier to log in to accounts than before they were using a password manager.
- Can be used on any account, including when 2FA is not used/available, but also when it is.
- Less likely to be phished, since users don't know their own passwords. When the browser won't auto-fill account credentials, a user may understand that this can indicate that they might be on a phishing site.
- It also helps prevent passwords from being reused after data breaches.
- Can improve the security of passwords on accounts that are shared with other users.
- Can be free, though paid models also exist.

Cons of using strong, unique passwords in a password manager

- Doesn't necessarily prevent phishing (e.g., when the password manager won't autofill the account credentials, the user can still copy and paste them into a phishing site).
- It's often time consuming and hard to set up and then requires consistent, repeated effort and buy-in.
- If the password manager is compromised, it serves as a single point of failure for all passwords.
- Requires the master password—i.e., the one that unlocks the password manager itself—to be strong, yet also not forgotten or lost.
- People may be locked out of accounts when the password manager is not available.
- Password managers are often designed, and easiest to use on personal, non-shared devices, which can be limiting in some cases.

Over time: Build a security culture

We believe that **one of the most effective ways to improve campaign security over time is to have as many people as possible who are involved with the campaign promote a security culture.** This encompasses all of the advice in this report and more. We believe every person on a campaign has a role to play in this, and can do so by encouraging others to turn on strong 2FA, sending around news articles about security, pointing out the other additional things people can do (especially as threats evolve), and making sure that when something suspicious happens, they report it to appropriate channels. All of this contributes to people involved with campaigns thinking about and acting on security and adapting to threats as they evolve.

In planning how to tackle the ambiguous goal of building a security culture, it's important to keep in mind that there is a limit to what people can realistically do, especially those whose top priority is winning an election on a short timeline with little pre-existing infrastructure. Technologists and IT staff should build and manage systems to handle as much security by default as is possible.

While building a security culture may sound like a daunting task, we believe that it can become more comprehensive over time as campaigns and the people who work on or with them adapt to the changing threat landscape. In fact, because of several highly publicized attacks in the political sphere many people involved with campaigns and political organizations already have an advantage that others may not have: awareness that there's a real problem. There are many ways to turn that awareness into a security culture. Next, we discuss a few.

No matter what size their campaign is or how much of a target they think the campaign may be, every campaign should get started with some very basic security resources, including knowing who to contact at the tech companies and party committees when they have a security question or suspect that they're being attacked. Having this information ready and available *before* an attack occurs should greatly help the campaign react quickly (and possibly mitigate or minimize damage) when and if an attack happens. These aims are often best supported by having a dedicated point-person for cybersecurity.

In the next section of the report, we discuss things that the cybersecurity point person can handle on their own. However they can also lead efforts which involve effort/cooperation from everyone—including:

- Developing policies for data handling and communications that everyone on the campaign needs to follow (e.g., where and how which types of data should be stored, and which platforms should be used for which types of communications).
- Setting up training to help everyone involved with the campaign understand the types of cybersecurity risks associated with campaigns today and what actions they should be taking to mitigate the risks (e.g., The USC Election Cybersecurity Initiative's training).
- Sharing/implementing the other ideas mentioned throughout this report.

It's very helpful when the impetus to build a security culture starts from the top, with candidates, campaign managers, and party leadership. If campaign and party leadership make cybersecurity a priority, everyone else involved with the campaign is far more likely to as well. Even if campaign and party leadership aren't emphasizing a security culture, anyone who is involved with a campaign can follow the advice in this report, follow up with additional advice from the more comprehensive guides, and spread the word to others who are involved with the campaign.

This is an ever-evolving process as campaigns bring in new staff, adopt new technologies, or see new or different attacks. Even if only some of these efforts towards a security culture occur, the campaign will be stronger, less vulnerable to attacks, and security awareness should increase (something that can also be useful for future cycles). We don't see the ideal state of a campaign being one where everyone involved with the campaign has security as their top priority, but rather one where everyone has reasonable awareness, develops practices and habits to help mitigate common risks for this population, and knows what to do or who to go to when something does happens, or even if they're suspicious of something.

Pros for a security culture

- Long-term, adaptable security improvements, across a range of best practices, by everyone involved in the campaign.
- Does the most to raise the bar for security by setting the campaign up to mitigate a broad range of attacks.

Cons for building a security culture

- Winning the election will likely continue to be a higher priority than digital security.
- No clear path to success; might be hard to implement a comprehensive cybersecurity program, at least before some practices become habit (e.g., given the transient nature of campaign staff, lack of up-to-date security knowledge, etc.).
- Takes awhile to reach full effect, without obvious, immediate improvement (e.g., it can be difficult to demonstrate how good cybersecurity practices prevented attacks, even when they did).
- Change can be hard - good security practices often compete with a "this is how we've always done it" or "I don't have time for that" attitude.

A recommendation for campaign organizations

Beyond advice for all people who are involved with campaigns, we firmly believe that campaigns should appoint someone to be their cybersecurity point person, or have access to a security expert / partner, perhaps provided by the parties' national committees. This role is important because it will help make cybersecurity more accessible and a part of the campaign culture. This point person may not have any background in cybersecurity or computer science more broadly, so they'd need to be provided with clear and easy-to-use resources. A very basic, v0-type set of resources could include:

- **Who to contact** should they need help with security (e.g., if they have questions, a suspected attack, etc.).
- **Pointers to training** (e.g., The USC Election Cybersecurity Initiative's training workshops) **and comprehensive guides** (e.g., Harvard Belfer Center's D3P Cybersecurity Campaign Playbook, the Device and Account Security Checklist 2.0, etc.).

Building on that very basic set of resources could be:

- An **incident response plan** for what to do if the campaign knows (or suspects) there has been an attack (e.g., something like the EAC's Cyber Incident Response Best Practices).
- Best practices for **what to do when someone leaves the campaign** (including passing along and updating account credentials, updating access control lists (ACLs), etc.).
- Best practices for **when to use which communications channels** (e.g., which platforms—email, encrypted messaging, text messaging, etc.—should be used for which types of communications) and how different types of data should be handled (e.g., where and how to store which types of data).
- Best practices for **setting up or auditing the campaign's security settings**, including G Suite / M365 and campaign-related social media accounts. This could also include setting up advanced security programs the tech platforms provide (e.g., Facebook Protect, Google's Advanced Protection Program, or Microsoft AccountGuard).
- A method to **test that the campaign's website is secure**, especially if it accepts donations, helps people register to vote, educates people about important voting information, etc. (e.g., think of what an attacker might do if they took over the website).
- A plan for **how to hand off the campaign information and credentials** to a future set of campaign workers for the next cycle.

For 2020, a v0 of this approach is probably the most that can happen. This can be improved later, but now seems like a good time to get something started.

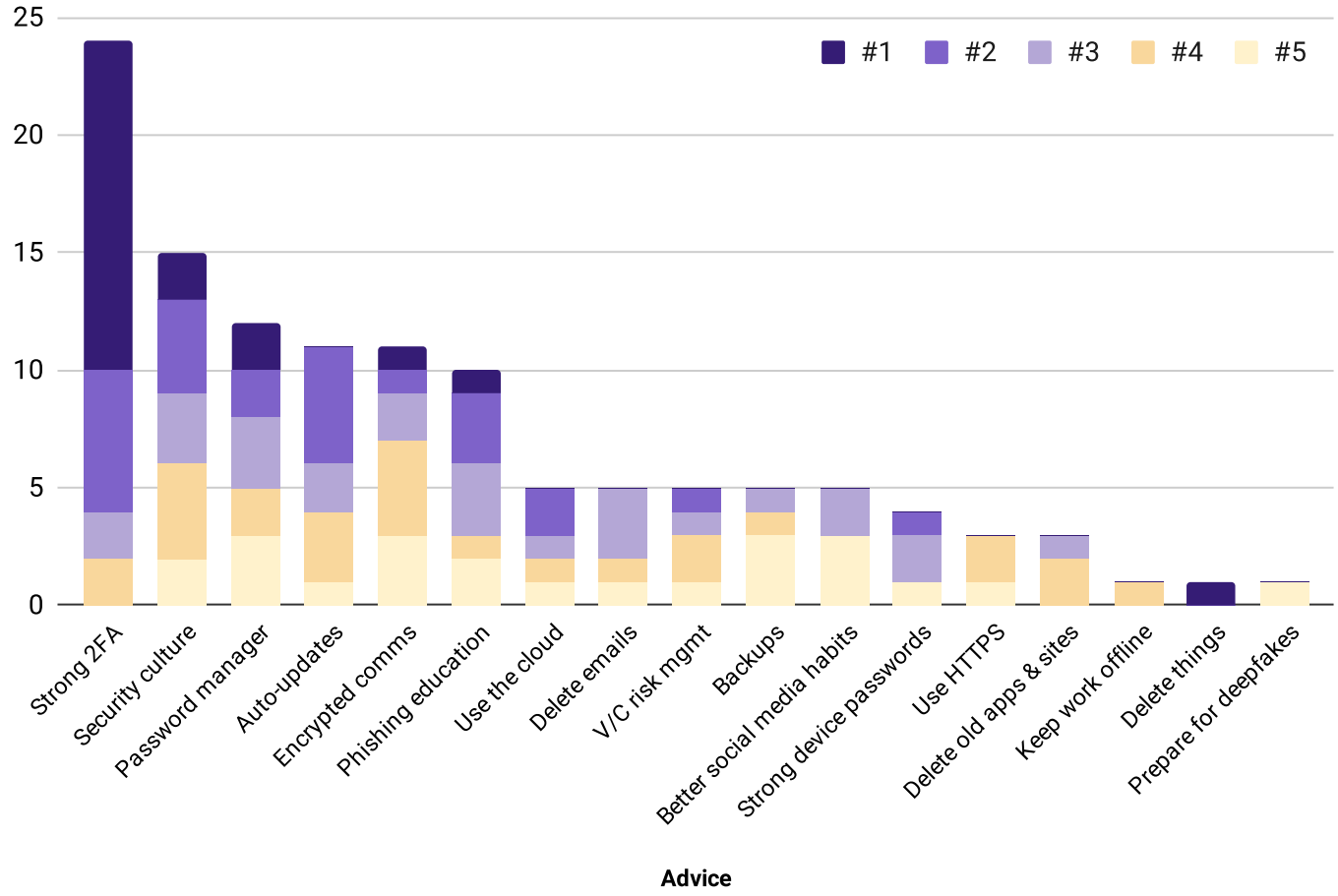
In the future, it's worth considering why someone would take on this responsibility—what's in it for them? After all, nearly everyone involved with a campaign already has too much to do. One idea was to establish a recognized "Cyber Fellow" program where they would be provided training and resources, and serving in this role would be good to mention on CVs. It's also worth considering how the role and recommendations might differ for campaigns of different sizes. The point person for a campaign with a staff of 5 probably doesn't have the time or need to implement all of the security advice that the point person on a campaign with a staff of 100+ does.

Methodology

Attendees. Forty-four people, not including the organizers, attended the virtual roundtable. It consisted of multiple meetings and tasks, including a kick-off session attended by 43 people, a work packet completed by 29, attending a small group discussion with 36 people attending one of 9 small groups, a final wrap-up session attended by 26, and contributing to / reviewing this report. Attendees came from 27 organizations, including 13 people from organizations affiliated with the Republican party, 12 from the Democratic party, 10 from technology companies, and 9 from academia and nonpartisan political nonprofits.

Work packet summary. Before the small group discussions, attendees completed a work packet where they reflected on what they thought the top 5 pieces of advice should be, in order of importance. Six pieces of advice were most commonly chosen as being in someone's top 5: (1) use 2FA; (2) establish a security culture; (3) use long, unique passwords in a password manager; (4 - a tie) turn on auto-updates for apps & devices *and* use encrypted communications; and (6) take phishing education. The chart below shows the top 5 ranked advice items from the 29 attendees who completed a work packet. For example, 24 attendees chose 2FA as a top 5 piece of advice, and they often ranked it as their #1 or #2.

Top 5 pieces of advice (N=29)



Small group summary. During the small group discussions, each small group decided on up to four pieces of advice, in order of importance, for people who work on / with / in support of campaigns. Most also discussed what the top recommendation for each campaign should be.

For the advice, we summarized the pros and cons from the work packets, with some additional information from the small group discussions. Every group spent some time discussing 2FA, while other pieces of advice came up in only some conversations.

8 of the 9 groups agreed with strong 2FA on the most important accounts. As well, 3 of the 9 groups agreed that each campaign should appoint someone on the campaign to be their cybersecurity point person, and a fourth suggested that the parties provide each campaign with access to a security expert/ partner, perhaps provided by the parties' national committees.

Other recommendations for campaigns from the small group discussions were to:

- Have an **incident response plan** for what to do in the event of a security incident
- Have an expert audit the campaign's G Suite / M365 settings as well as the settings for any campaign-related social media accounts
- **Secure the campaign's website** (especially if it accepts donations, helps people register to vote, educates people about important voting information, etc.)
- Develop **policies for data handling** (e.g., where and how to store which types of data) **and communications** (which platforms should be used for which types of communications)
- Have a policy / know best practices for what to do when someone leaves and/or the campaign ends
- Lay the groundwork for establishing a **stronger security culture** in the future

Acknowledgements

A **very big thank you** to all Roundtable attendees, assistants of the attendees who helped coordinate sessions, research participants, and the many people at Google who helped make the research & roundtable happen!

APPENDIX A **Sample advice text**

Below are 4 options for a *primary message* (which is likely to be a tweet, or compiled together in an email or Signal/Wickr/Slack message). The *secondary, follow-up messages* could accompany any of the primary message options. Please customize the text as appropriate.

Primary message options

Option 1 (basic) — Primary message

For people working with a political campaign: on your most important personal and campaign accounts, only use the strongest form of Two-Factor Authentication (2FA) available, ideally hardware security keys.

Option 2 (your responsibility) — Primary message

For people working with a political campaign: only use the strongest form of Two-Factor Authentication (2FA) available, ideally hardware security keys, on your most important personal and campaign accounts. This protects you and the campaign, and is a meaningful step to protect democracy.

Option 3 (foreign governments) — Primary message

People on political campaigns are being targeted by foreign governments and need to use the strongest form of 2FA—hardware security keys—on their most important personal and campaign accounts to protect themselves, the campaigns, and democracy.

Option 4 (specific countries) — Primary message

People on political campaigns are being targeted by [[country]], and need to use the strongest form of 2FA—hardware security keys—on their most important personal and campaign accounts to protect themselves, the campaigns, and democracy.

Secondary, follow up messages (pick and choose, or share them all!)

By *most important accounts*, we mean to start with your personal and campaign accounts for email, social media, and banking.

Even if you have some form of 2FA on those accounts already (and we hope you do!), it's a good idea to verify that you're using the strongest form. If you aren't, it's time to upgrade [[if applicable: Reach out to the DDC to see if your campaign qualifies for free hardware security keys]].

With Two-Factor Authentication (2FA), when you try to log in to your account, especially on a new device, you will be asked for your password + something else to verify that it's really you. This might be a hardware security key that you tap (recommended), or a one-time code you type in (often from an app or SMS).

There are many different types of 2FA. Hardware security keys offer the strongest protection—*by a lot*. Shown are some common factors, ordered by how much they can protect people working with political campaigns. *[[see graphic in Appendix B]]*

If the site allows it, turn off the ability to fall back on weaker 2FA options (like SMS codes). This will stop attackers from using your backups to access your account. Get an extra hardware key to use as your backup, or save backup account codes as your fall back.

How to turn 2FA on [[suggestion for a company that has it, e.g., Facebook says turn on 2FA and here's how to do it on Facebook]]

If hardware security keys aren't an option for you, or while you're waiting for yours to arrive, make sure you're using some form of 2FA, like getting a code from an app or even a text message on your most important personal and campaign accounts. Since you're at higher risk than the general population, having a second factor—even if it isn't the strongest—is better than nothing.

APPENDIX B **Sample graphics**