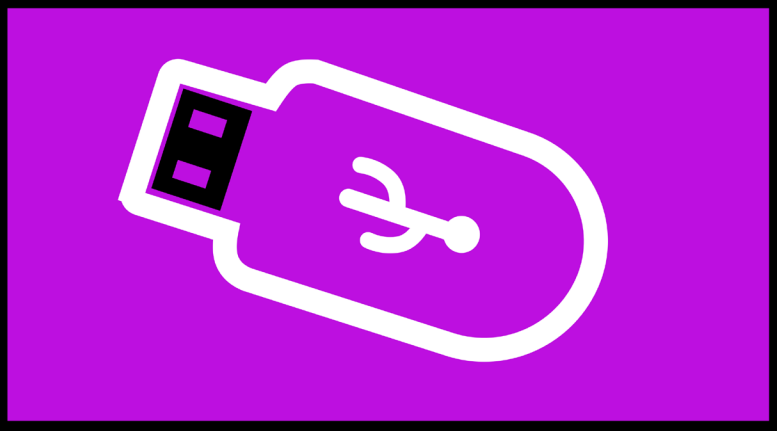
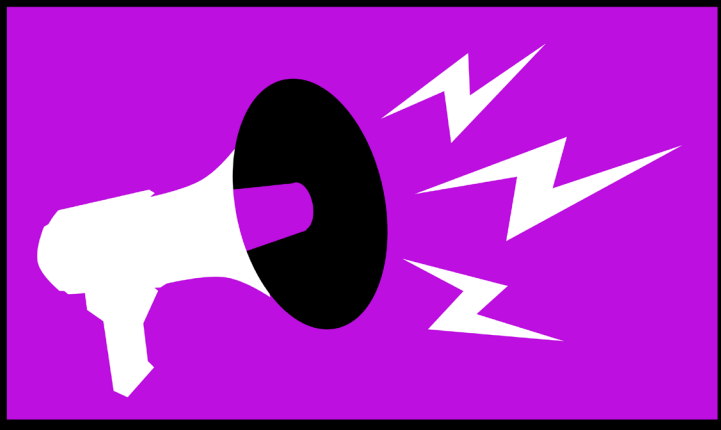
Tech Yourself

A Tech Framework Guide for Progressive & Democratic Candidates

ISSUE 8

Light Cybersecurity Guidelines





Learn how to run a digitally savvy campaign!

TechYourself

A Framework Guide for Candidates on How to Use Tech to Win Campaigns

Light Cybersecurity Guidelines

How to best protect your campaign, team, and assets from harmful cyber attacks.

www.techyourself.org

Illustrated by Daniel Scannell

Light Cybersecurity Guidelines

We could not release a tech framework guide without including some references on how to run the safest campaign you can. This section will arm you with a simple frame of reference and checklist to implement basic cyber vigilance in your organization. This list will also enable your organization to demonstrate its progress toward goals in implementing basic cyber hygiene, and we will delineate between what type of security can reasonably be expected based on your organization's size and resources. There are three areas where you have to implement basic cyber hygiene in your campaign: individuals/volunteers, your enterprise itself (the campaign and it's assets), and your employees/staffers. Before we examine those, let's quickly examine the most typical types of attacks that can happen.

How Big a Deal Is Cybersecurity?

In most small to midsize companies, cyber risks can be very theoretical. You have some exposure from bad actors who are scanning networks all the time looking for vulnerabilities, but very few who are concocting attacks aimed for you.

That's not true in politics. You not only have to deal with those threats, but you have to deal with opposition attacks. Bear in mind, these attacks are not necessarily coordinated by an opponent directly but are still executed for their benefit by overzealous supporters or fame seekers. You also have to deal with directed attacks by foreign governments. This isn't just tin foil hat talk - foreign government attempts at interference aren't new and aren't limited to presidential campaigns. If you are running for anything above band ,1 it's virtually guaranteed that you'll be attacked not just by "script kiddies" but by well-trained professionals with years of cyber warfare experience.

And the consequences of an attack are not trivial. They can include the inability to take donations, the destruction of your valuable data, the rewriting of your site to include false claims, and much, much more.

Common Types of Cyber Attacks

Bad actors have a variety of ways to make your life miserable. Here are a few of the most common and how they translate to campaigns.

Phishing and Spear Phishing

You might be familiar with "phishing" attacks. These are often spread via email, or on social media, and involve fake communications- think Nigerian Prince needs your help to handle his money- to capture credit card information or logins. Spear phishing is a variation where the communication is highly customized to the individual, often seeming to involve a company or person with whom they regularly communicate.

For political campaigns, there are two worries. The first concern is the same for consumers and candidates; phishing will lead to a malware installation that attacks personal information or the staff or volunteer machines. The second is that someone will send emails purporting to be from you with false or misleading information.

Malware is malicious software that can spy on you, screw up basic functions, or even hold your entire

computer for ransom. In political attacks, the intent is often to spy and/or transmit data from the hard drive to someone outside the network; in rare cases, it is also used to disrupt the entire system and take the computer down entirely. In smaller campaigns, usually every machine has access to all the tools and data, so any user can be attacked with disastrous consequences.

Eavesdropping

Eavesdropping attacks can also happen if a hacker interrupts traffic between you and a new network. If you use Starbucks wifi, for example, your information passes to their network as you work. A hacker can get in the middle of this and see everything you or a team member is doing- if they choose. It's also worth mentioning that eavesdropping is even more common between people. If you are having a conversation in Starbucks, in an Uber, or waiting for a plane, remember there's a 50/50 shot that anyone within earshot supports your competitor and just might have a way to use anything they hear.

Denial of Service

DDOS attacks are slightly different. DDOS stands for "distributed denial of service" and uses a bot methodology to "flood" a server or network. A real world example would be sending 100,000 people to an airport to flood the ticket lines so real people can't check in to board their flights - it's much easier to do this in the online world. If your site is dealing with someone asking it the same question three million times a minute, it won't fulfill basic functions for other users, such as bringing them to the donate page. DDOS attacks often happen at key points- like when you need donations, the day before an election, or the day a primary is won and the contender is announced.

Data Poisoning

One type of attack that is relatively unique to political campaigns is data poisoning. What this means is that there is an attempt- either automated or manual- to corrupt your voter file. For example, this could happen if a "volunteer" (really a hostile actor or even an incompetent user) uses a call tool and marks every persuadable voter as dead- causing your campaign to stop contracting them.

Other

These are not the only types of political hacking. In 2016, there were direct attacks on voting machines, a DNC server that was transmitting information directly to Russia, a phishing attack that targeted (and fooled) John Podesta and his team, an alleged DNC attack by two Russian groups called "Cozy Bear" and "Fancy Bear," a Wikileaks hack, a personal posting of phone numbers of various members of the Democratic Congress, and many more. You can read more here.

Individual and Volunteer Security Tips

Humans are ALWAYS the weakest point of the network. Training can be helpful, but you have to ensure security happens regardless of whether employees follow the protocols. For example, the senior leadership in one of the top U.S. Military Commands went through a training series several years ago to train them to avoid phishing attacks. To test the training's efficacy, the NSA sent each of the chiefs an email that read "This is a phishing attack" in the subject line. All of the chiefs- 100% of the top leadership- clicked on the malicious link. If training has no impact on even these senior military leaders who understand the threat, then we must assume anti-phishing training will be of little use in stopping nefarious actors. It's a good idea to take security out of

the staffs' hands as much as possible. The New York Times and the National Institute of Standards and Technology have outlined the following steps as effective cyber hygiene. These steps need to be sent immediately to your team at the beginning of a campaign, as they can ensure hacks of personal information are less likely. This section has singled out the steps most immediately relevant for a campaign, and all campaigns in bands can benefit from making sure their team gets these notes in an email.

1. Secure Message Apps: A candidate, their circle, and the campaign staffers should use a default messaging app like Signal, Wickr, or WhatsApp for messaging within their team. Signal is a direct IM app, and Wickr is more like Slack- enabling a team that is virtual to communicate in a room with various channels. SMS messages are not secure or encrypted by default and are especially vulnerable if a phone is lost or stolen. Many messaging apps can also automatically delete messages after a certain period of time, which is very good. Fewer messages stored at any one time means fewer that can be hacked. Signal has also made its code is open source, meaning it is examined by third-party cybersecurity experts regularly. At bands three-five, using these tools is highly recommended.

2. Pfishing/Suspicious Emails: Despite training's limited success, staff should be expected to use caution when clicking on the links or PDFs in emails. If you are not sure about something, don't clink. Each email should be approached with caution, with the user double checking the outgoing email address before clicking. Be aware that hackers might aim at personal fears. If you get an email about your kid or your kid's school as a mother, for example, make sure to double-check it. This example is a popular opening line for attacks aimed at women.

3. Backup Data: Information should be backed up in the cloud and encrypted. If a laptop is stolen or hacked, files on the laptop can be accessed in their unencrypted form with little effort. Keeping data in AWS, Google suite, or other similar cloud based systems is simple, inexpensive, and secure. CIO magazine offers these five tips on how to keep data secure in the cloud.

4. Two Factor Authentication: All major tech platforms (like Google/Gmail, Facebook, Twitter, and Apple) support a system called two factor authentication (sometimes "2FA", "TFA", or two-step authentication). The basic idea is that in addition to a password, you need to be able to receive a text message with a verification code in order to log in to these systems. This means that even if your password is guessed or stolen, your account is very difficult to compromise without also having access to your phone. Increasingly, political tools either support logging in with Google or Facebook or have some form of 2FA. Simply insisting employees keep their two factor authentication turned on is another simple and free practice to dramatically improve security in the organization. G Suite also allows the system administrator to force all users to enable 2FA, which is a strongly recommended practice. More on this is here, if needed, from PC Magazine.

In addition to the steps above, the following steps are a bit more campaign specific:

5. Don't Write Things Down: Maybe the most important cyber defense is implementing the "Washington Post Rule," which is not to put things in writing that you don't want on the front page of the Washington Post. Never use post-it notes or memos for

things that need to be secure or leave clear visuals of something sensitive in your office The above list should protect any campaign staff from hacktivists or more sophisticated hackers that are scanning thousands of campaigns looking for vulnerabilities to exploit; however, no amount of time or money can stop all of the hackers all of the time. Staff, candidates, consultants, and interns should regularly be reminded that if they do not want something on the front page of a paper, don't write it down. Don't print it, as even a few minutes of lag time sitting at an office printer can be dangerous. Pick up the phone or walk down the hall and say it verbally, send it through an encrypted channel, or don't say it all. Keep in mind too, that it's very common for bars in DC - and around the country- to have activists and campaign staffers around all the time. It's not only possible, it's likely anything you say over a drink will be heard. This critically important cyber security practice can be reinforced by management insisting staff call or visit them to discuss an issue whenever a long or inappropriately worded email or text is sent. Phone calls are always better, as it leaves less of a trail for a hacker to follow and grab information from. Unlike the phishing training that seemed to have little effect on the Joint Chiefs, "Washington Post Rule" training does seem to have an effect if senior leadership in the organization is disciplined about implementation.

6. Use Good, Unique Passwords (and a Password Manager.) When you register for any tool, you are giving them access to your password. While the best practice is for the providers not to store your clear text password- they should do one-way encryption called "hashing" so that even if their systems are hacked your password will be safe-, that's not always done. You've probably seen articles about passwords being stolen from big companies, and, if your password is one of these, you might find the thieves try your password out on all kinds of other sites. The best ways to protect yourself are 1) use strong, hard to guess , but easy to remember passwords (including upper and lower case letters, numbers, and punctuation); 2) don't reuse passwords on multiple sites; and 3) use a password management program like 1password, LastPass, or Keeper to securely store your passwords, so you don't need to be able to remember them.

7. Use an Anti-Malware Package. Yes, even Mac users should do this since, despite a historically better record on anti-malware, there have been a number of successful attacks on all platforms. Many anti-malware packages like ClamAV and MalwareBytes have free versions.

8. When Possible, Use iPhones. While Androids are great devices and can certainly be hardened to deal with security risks, if you are dealing with tech novices iPhones are more secure out-of-box.

Campaign Network Hygiene

Now let's talk about how to keep your campaign safe. Smaller campaigns, like those in bands one, two and three, can simply operate on Google or Microsoft suites as these programs are easy to use and provide strong back end security if they are properly set up. However, as you run for larger and larger races, you need to realize when your organization grows from a few people sharing Google Docs to an enterprise network. Once you enter bands four and five, the CIS 20 Critical Cyber Security Controls is "the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks." And, once in bands four and five, you really need to have an IT professional on contractor hired to maintain your systems. Accept the reality of

today and build that into your budget.

The top five of their 20 Critical Cybersecurity Controls, have been repeatedly shown to mitigate against 85% of known threats. This list is maintained by a group of the foremost cyber experts from industry, government and academia quarterly. These five best practices include:

1. **Inventory and control of hardware assets:** "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." This means an organization must identify all the physical assets on its network, like printers, laptops etc. and identify any that are unapproved. This is particularly relevant with the dramatic expansion of IoT. For example, the massive hack against Target was executed through a refrigeration device connected to the network. Its likely the security department didn't even know the device was connected to the network.

2. **Inventory and Control of Software Assets:** "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution." This guideline builds off the first. Once one knows all the hardware assets on their network, they must also identify what software is running on those assets to decide if any of it is unauthorized or malicious.

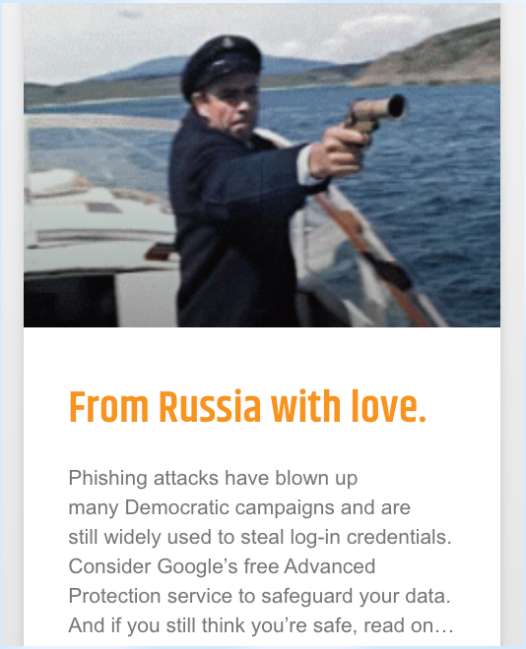
3. **Continuous Vulnerability Management:** "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers." This control requires one to have tools in place that continuously scan your network for vulnerabilities and subsequently ensure someone fixes them. Most IT staff or contractors can accomplish this with free/inexpensive tools.

4. **Controlled Use of Administrative Privileges:** This is "the processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications." For example, systems like VAN have different layers of access to ensure no one has more access to the network than they need or is assigned to them. Some people refer to this control as the "Snowden Control." Snowden was able to hack vast swaths of the NSA network because he gave himself greater and greater administrative privileges over the network to get access to the data he wanted.

5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** "Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings." Even if all campaign hardware and software is configured to be secure out-of-the-box, staffers should continue to update software. This again is an activity that an entry level IT staffer or contractor can accomplish. For example, ensuring that devices, like printers, are not connected to web-servers ensure only a limited number of machines are directly connected to the Internet. Thus, the network as a whole is more secure.

6. **Domain Registration:** Make sure that someone hasn't registered a domain name similar to your campaign. This is called domain-squatting and is dangerous because unsuspecting individuals who mis-type your web site address are directed to a fake website where they may be tricked into making a donation or worse. Learn more here.

7. **Protection:** Use Google's Advanced Protection service so that you are protected with two factor authentication even if your passwords are stolen. More details here.



8. **DDOS Attacks:** Protect against DDOS attacks with cloud-based platforms like Fastly and Cloudflare. DDOS attacks are when a bot repeatedly pings your site, trying to slow it's load time, or bring it down. This can make or break a campaign, especially if your site goes down the day before an election, taking donation capabilities with it.

The above is for full time staffers and employees, so you can have lighter approaches when it comes to attending a conference, or other election-based events. But even there, use common sense. Should your team be sitting in a Starbucks using that wifi if you are at a convention where there' a significant amount of campaign staff from Left and Right campaigns? Maybe not. All it takes is one person to hack into the cloud of a staffer and get an inappropriate picture, for example, and you have an issue.

Your IT staffer should implement this as a frame of reference by which she can report to you on progress toward implementation of these goals. Hold them to goals as you would any other team member. The above list is akin to the reporting protocols a campaign uses to measure the field director's performance based on a hand-ful of key metrics, like how many voter contacts, volunteer sign ups and house parties they have completed each

week. Similarly, you should take this list to your lead cyber person and ask them if they can answer all of these questions with specificity like, "We have 32 physical assets on our network and 18 types of software running on the network, which include yadda yadda. We also have 27 out of our 34 staff using Signal as their default messaging app." If all these controls aren't in place, and they surely are not, direct them to give you a timeline and plan for implementation. The cyber lead for an organization should be treated just like the field director or finance director with specific goals and reports that are delivered regularly. Don't be intimidated to ask these questions. Remember, you didn't come up with this list. The NSA and leaders in the tech industry did. NSA, DOD, DHS, JP Morgan, Citibank, Google, Amazon, etc. place such a high priority on the above controls they collectively spend tens of billions annually to implement them. If your network administrator isn't trying to implement them as well, they are failing.

Staffing Controls and Staying Vigilant

While attempting to implement the basic cyber hygiene above, an organization will quickly realize the most difficult challenge in cyber security is a lack of qualified staff. In fact, there is a 350,000 person shortage in cyber professionals nation-wide. This number is expected to grow to millions in the next few years. Some of this ties into a lack of high school and college students learning coding, and some of this ties into the fact that hackers are labeled hackers for a reason---a lot of them don't choose to work for anyone but themselves.

In the Voting Machine Hacking Village at DEFCON, the world's largest hacker conference, the hacker and security community have a deep passion for politics and democracy. Many of them are quite progressive as well. Those unsure may be able to take a page out of the 2016 Bernie Campaign to hack the workforce challenges in cyber security. Bernie had a widely successful program called Coders for Bernie, where the campaign was able to access the dearth of cost prohibitive progressive leaning coders by finding creative ways for them to volunteer for the campaign using their unique skills. Coders for Bernie helped build campaign apps, improve efficiency of digital tools the campaign used, and implement basic safety. Obviously, some management and oversight was needed, but the campaign received more human hours of programming support than it could have ever dreamed of buying.

While people may find it counterintuitive to use volunteers for something as sensitive as cyber security, the simple fact is you will probably not find qualified people to do this work for a price you can afford. Without people who can do this work, you won't be able to do security. Further, the campaign is free to require all cyber volunteers to clear the same background investigation staff must pass. These volunteers would be vetted at the same level as if you hired them. Modifying the Coders for Bernie program to something like "Hackers for (insert your candidate or cause)" may be your best shot at finding someone who can help you do security.

It's a crazy time, and with time-strapped campaigns, especially those in bands one, two and three, it can be easy to think that you might fly under the radar with regard to implementing some of these guidelines. Try not to assume that. There are crazy stories out there. From pictures being taken from icloud and becoming time bombs for candidates that don't want them released out of context and website donation pages going down the day before an election to local election officials getting hacked on site as voting happens. While some hacking is very overt, and will throw your staff into a panic, sometimes it is more subtle. If you feel something is off, it very well might be. Implementing these practices is all your organization can reasonably be expected to do to secure itself against attack, but add a healthy dose of monitoring and suspicion as well. These steps are akin to protecting your home by adopting a big scary (rescue) dog, installing a (union certified) alarm system and leaving a (solar battery powered) light on at night. The bad guys could still get around your defenses if they were determined. However, you have made it difficult enough using the tactics above, that they will likely just move on to your neighbors' house, who likely has the front door and all the windows wide open.