SECRETARY
KATIE
HOBBS

Cybersecurity tips for candidates, parties, and PACs

Arizona Secretary of State

ABOUT THIS PACKET

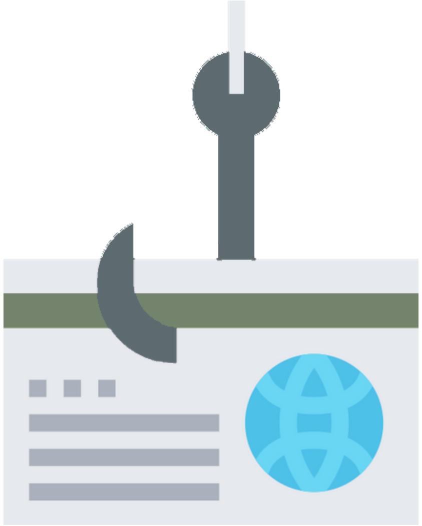
In today's environment, political entities have become high value targets for hackers and others that wish to disrupt the election process. These bad actors can include nation states, political opponents, hacktivists, or profiteers. The Arizona Secretary of State's Office is committed to providing fair elections across the 15 counties of Arizona, and in response has prepared this guide to assist candidates and political entities with keeping their information and accounts safe. In this document, we've assembled best practices from leading sources around the country that can help secure your political message.

TIP #1: USE TWO-FACTOR AUTHENTICATION FOR ALL SERVICES

Two-factor authentication increases security by requiring two separate validations in order to log in. This makes it significantly harder for an intruder to gain access even if a device or password is stolen. For instance, after entering your password, Twitter can send you a text with a special code that you also need to enter to successfully log in. In this way, a bad actor would need your phone AND your password to be able to log in as you.

We recommend using two-factor authentication for social media accounts, email, and website editing access. Here is a fantastic list of web services that support two-factor authentication: twofactorauth.org.

TIP #2: BE PREPARED FOR PHISHING ATTACKS



Phishing is a technique where a bad actor sends realistic-looking emails that encourage the recipient to click on a malicious link or attachment. Once clicked, the bad actors can gather private information or leave spyware or malware on your computer. It is estimated that over 90% of successful hacks start with a phishing email.*

Campaigns have been targeted by extremely well-crafted and personalized emails that have successfully led to hacking. Everyone in your organization should learn how to identify phishing emails. We also recommend testing your staff's phishing resilience by using a phishing testing service that sends them harmless phishing emails.

*Verizon Data Breach Investigation Report (2017)

TIP #3: PROTECT YOUR SOCIAL MEDIA ACCOUNTS

A real problem with social media is bad actors creating copycat accounts and passing along their own messaging under somebody else's name. A verification badge appears on accounts that have been proven to be authentic so that the public can be assured it is real. The process to get this is different for each company, but a quick web search will get you the instructions.

Social media can be the catalyst that quickly spreads false or misleading information. In order to make it easier for social media companies to remove this content, it is best to establish points of contact early, or bookmark pages that will help you recover your account or report misinformation. Preparedness counts at election time!

TIP #4: SECURE YOUR MOBILE DEVICES

It may seem obvious, but make sure cell phones, tablets and laptops are using passwords, security patterns, or biometric security. Also make sure they are timing out so they lock after not being used for a while.

An unlocked device in the wrong hands can be the key to the kingdom. Critical mobile devices should store their data in an encrypted format so that even if somebody gets into it, the data will be of no use.

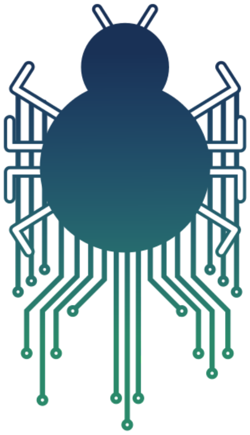
Have a pre-made plan about what to do if you lose a mobile device. Do you know where to go to remotely wipe it? Only use dedicated and secure Wi-Fi networks at campaign offices, and use secure mobile Wi-Fi hotspots when traveling. And finally, just like home or office computers, make sure your mobile devices are patched and updated regularly.

TIP #5: PAY ATTENTION TO PASSWORDS

Different passwords should be used for different accounts to ensure that one breach does not give a hacker access to every account.

You should use long passwords which are tougher to break. As well, consider using a password keeper program to securely store your passwords and to generate complex, hard-to-break passwords.

TIP #6: HAVE PROFESSIONAL HELP STANDING BY



Cyber incidents never seem to happen at convenient times. So if it's Election Day and your organization is experiencing a cyberattack, it may already be too late to find a cybersecurity contractor to help you.

The best bet is to make arrangements ahead of time, and have the number to call ready to go. As well, if you have an extensive office network, you may wish to have a security expert assess the vulnerabilities and make recommendations about shoring up your defenses before there is a problem.

TIP #7: USE ENCRYPTED MESSAGING APPLICATIONS FOR SENSITIVE CONVERSATIONS

It's vitally important for political entities to keep their private conversations private. There are several products available that can encrypt your messages and documents before you send them and un-encrypt them on the other end. This can stop bad actors from being able to read your messages if they are able to intercept them. These products can be installed on all types of devices, from phones to office computers.

TIP #8: CONSIDER CLOUD SERVICES VS. ON-PREMISE SYSTEMS

The cloud refers to services that offer an online platform to store data, send email, or host websites. In most cases (and when used in conjunction with two-factor authentication), these services are more secure and easier to implement than systems that we can build at our offices. Additionally, they ensure that loss or damage of a single device does not lead to data loss.

TIP #9: PROTECT YOUR WEBSITES

Your website should be behind a Web Application Firewall (WAF) or similar protection. These services protect your website from certain types of attacks, including Distributed Denial of Service (DDoS) attacks that can shut down your site for extended periods of time. There are free options for this, including Project Shield by Google.

As well, carefully monitor who has access to edit your website and only grant permissions to those who absolutely need it.

Hire a service to perform penetration testing on your websites, so you can know if there are security concerns and address them.

TIP #10: KNOW AND UTILIZE AVAILABLE CAMPAIGN SECURITY RESOURCES

- **FBI – Protected Voices Initiative**
  www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

- **Cybersecurity Campaign Playbook. Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2017.**
  www.belfercenter.org/CyberPlaybook

- **U.S. Dept of Homeland Security**
  Offers several services, including phishing testing and cybersecurity assessments - nicc@hq.dhs.gov "Campaign Checklist,"

  dhs.gov/sites/default/files/publications/DHS%20Campaign%20Checklist_FINAL%20October.pdf

- **Google – Advanced Protection Program**
  https://landing.google.com/advancedprotection

- **Google – Protect Your Election**
  Programprotectyourelection.withgoogle.com/intl/en

- **Microsoft - 365 for Campaigns**
  https://m365forcampaigns.microsoft.com/en-us/