
EDF ACTION CAMPAIGN ACADEMY
EDF ACTION
Advocacy partner of Environmental Defense Fund
CAMPAIGN ACADEMY

D3P: WHO WE ARE

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Google

CROWDSTRIKE

Jigsaw

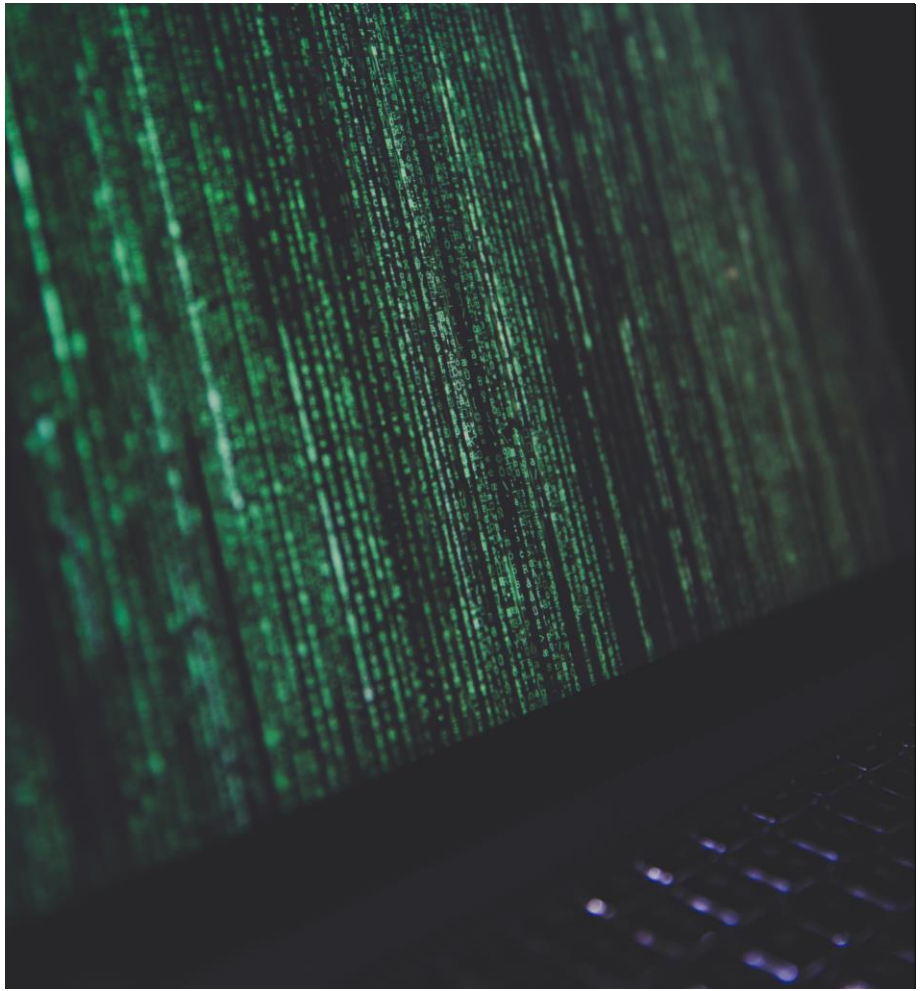
D3P: WHAT WE DO

- **Help those on the frontline—campaigns and election officials—** understand the risks they face from cyber and information operations
- **Provide practical "playbooks"** to improve readiness
- **Emphasize training and preparedness** as fundamental to success—a plan is only as good as its execution
- **Empower policymakers** to better understand the issues

BELFERCENTER.ORG/CYBERPLAYBOOK

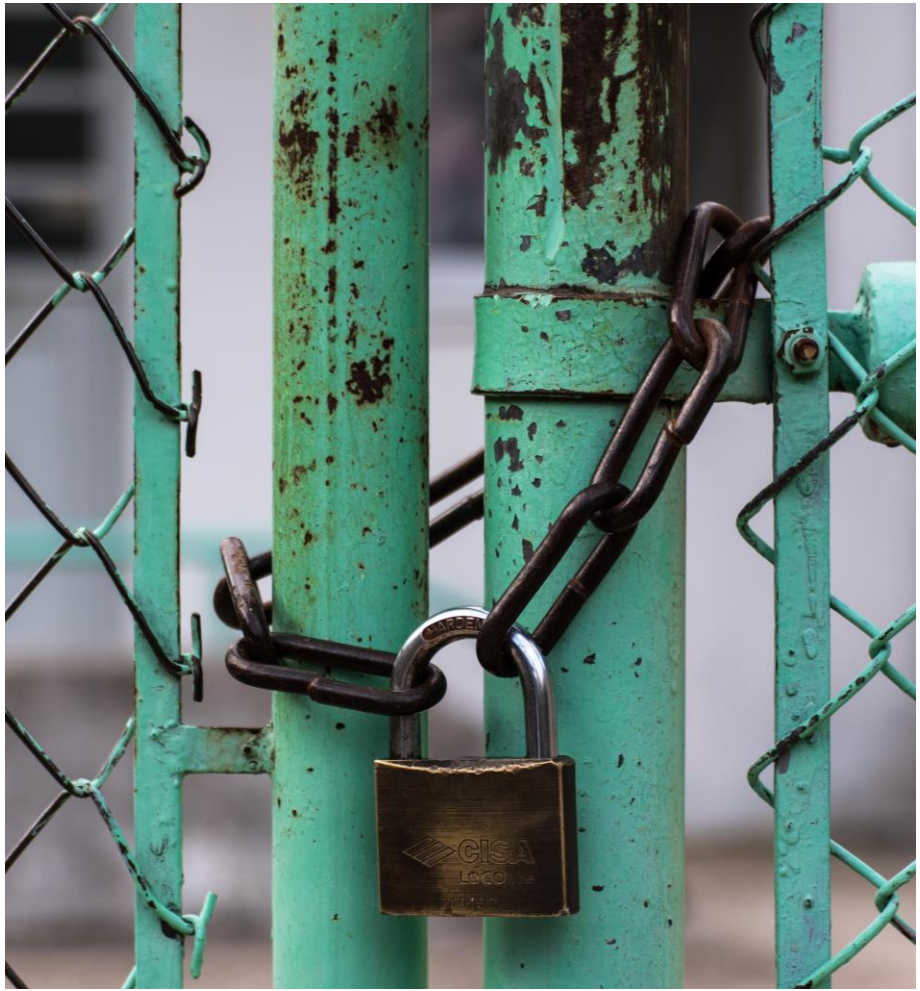
THE THREAT

- Nation states
  - Russia
  - China
  - North Korea
  - Iran
- Cybercriminals
- Black hat hackers



THE CAMPAIGN ENVIRONMENT

- Soft targets
- Temporary and transient
- Lack of resources (time and money) to devote to security
- Little time for security training for staff
- Proliferation of BYOD (bring your own device)
- Wealth of proprietary information and sensitive documents



CAMPAIGN PLAYBOOK: TOP FIVE CHECKLIST

1. Set the tone

2. Use the cloud

3. Use two-factor authentication (2FA) and strong passwords:

4. Use encrypted messaging for sensitive conversations and materials

5. Plan and prepare

THE RISK

- Vulnerabilities: weaknesses in your campaign that make information susceptible to theft, alteration or destruction
  - Hardware
  - Software
  - Processes
  - People
- Capabilities and intentions of bad actors
- Ease of access to networks and data of interest
- Proliferation of internet-connected devices

CAMPAIGN PLAYBOOK: TOP FIVE CHECKLIST

Prepare: Create a culture of security vigilance that minimizes weak links. Establish clear ground rules that are enforced from the top-down and are embraced from the bottom-up.

Protect: Prevention is critical. Build the strongest defenses that time and money allow is a key part of reducing risk. A few basic security measures used in combination can make a campaign's digital architecture more difficult to breach and more resilient if compromised.

Persist: Campaigns now face adversaries with ever-increasing levels of resources and expertise; even the most vigilant culture and the toughest infrastructure may not prevent a security breach. Campaigns need to develop a plan ahead of time on how to deal with a breach in the event that one occurs.

STEPS TO SECURING YOUR CAMPAIGN

- Establish a culture of security as a standard for a winning campaign
- Thoroughly vet staff, volunteers and interns
- Require use of secure email and storage by consultants and vendors
- Control access to online services
- Educate staff about phishing threat
  - Think before you click!

Step 1: The Human Element

STEPS TO SECURING YOUR CAMPAIGN

- Use a cloud-based office suite for secure email, chat, file sharing, document creation
- Use secure systems for communications
  - Encrypted messaging
  - Disable archiving for messaging services
- Defend your email
  - Turn on auto delete
  - Retain emails for one month or less
- Secure personal accounts

Step 2: Internal Communications

STEPS TO SECURING YOUR CAMPAIGN

- Require two-factor authentication
- Require strong passwords
- Use a password manager
- Create separate accounts for administrators and users
- Conduct periodic reviews

Step 3: Account Management and Access

STEPS TO SECURING YOUR CAMPAIGN

- Use the most updated operating system (OS)
- Use an automatic cloud-based backup service
- Establish device use policy
- Change default passwords and settings
- Require encryption on all devices

Step 4: Devices

STEPS TO SECURING YOUR CAMPAIGN

- Store data on cloud services
- Have a separate guest wifi account
- Avoid use of public wifi services
- Secure your browser

Step 5: Networks

STEPS TO SECURING YOUR CAMPAIGN

- Information Operations are a communications problem
- Know what's going on
- Establish contact with key social media platforms and notify them if you find fake or misleading information
- Monitor for imposter sites
- Protect Against a Distributed Denial of Service Attack (DDoS)

Step 6: Information Operations and Public Facing Communication