Don't Let Your Family or Your Campaign Fall Victim to Cyber Criminals

Key Points for Elected Officials and Candidates
Cyber security might seem like an IT issue, but a security breach is a political flashpoint. Most cyber security experts agree that public officials are high-value targets and should adopt a "not if, but when" attitude towards cyber security breaches.

Five things to do that will make you a harder target for cyber criminals.

- Recognize that you, your family and your campaign staff and volunteers are targets.
- Identify and define expected uses for all of your information technology, social media, and online assets for campaign members and volunteers.
- Create policies or procedures that identify how technology is to be used, how data is to be stored and shared, and provide training for applicable staff members.
- Use strong, complex passwords for all smart phones, email accounts and IT systems. Use multi-factor authentication for all connected devices and accounts that support this security feature.
- Install and keep anti-virus tools up to date on all computer systems and use spam and junk mail filters in email services that scan emails for viruses or known spam or malicious content.

Who poses a threat to cybersecurity?

- Scammers and thieves seeking information and advanced persistent threats (APTs), which are sophisticated, well-resourced attacks, usually backed by political or financial motivation.
- Individual hackers or hacker collectives seeking fame, profit or publicity for activist agendas.
- International state-sponsored criminals who want to disrupt operations, create an atmosphere of fear and uncertainty, or steal sensitive information for profit or espionage.
- Disgruntled employees, contractors and other insiders who aim to leak, steal or sell classified information.
- Employees that inadvertently aid cyber thieves by falling for scams.
- Organizations practicing poor security management, leading to non-malicious attacks or data leakage.

What are the biggest targets/risks?

- Sensitive public safety information.
- Intellectual property and security intelligence.
- Constituent information, which can include:
    - Names and addresses.
    - Personal identification numbers, including Social Security, passport, driver's license and taxpayer identification.
    - Date and place of birth.
    - Mother's maiden name.
    - Telephone numbers.
    - Photographs.
    - Financial records, including bank account and credit card numbers.
    - Employment information.
- Email, text messages and confidential communications.
- Donor or contributor lists.

Bottom Line: Lead by example. You are responsible for doing everything you can to protect your constituents.

Mark Gower, State Chief Information Security Officer and CyberCommand Director, OK • Agnes Kirk, State Chief Information Security Officer, WA • Kirk Lonbom, Acting Secretary of the Department of Innovation and Technology, IL • Elayne Starkey, State Chief Information Security Officer, DE • Joe Acosta, State Chief Information Security Officer, KS