CYBERSECURITY BEST PRACTICES

Questions or Issues? See it, say it. Email: security@vademocrats.org

EMAIL SECURITY

Remember, email is inherently insecure. Never email sensitive information, such as passwords or personal information like credit card numbers, passport numbers, social security numbers and birthdates. DO NOT open attachments or click links in emails unless you know the sender and are expecting it. If in doubt, contact the sender (not over email in case their account is compromised). Do not let staff use personal email for official campaign business (using personal accounts put both the staff member and the campaign at risk).

TWO FACTOR AUTHENTICATION

Enable two factor authentication (2FA) on all accounts. Use twofactorauth.org to see which services support 2FA and how to enable it. Some of the highest risk accounts on which you should enable 2FA are (check them off below as you enable 2FA):

- ○ Gmail / Email account(s)
- ○ Dropbox
- ○ Apple ID (iCloud)
- ○ Twitter
- ○ Facebook
- ○ Office365 / OneDrive
- ○ Your bank account(s)
- ○ Amazon.com
- ○ LinkedIn

PASSWORDS

Use a password manager like LastPass to keep track of your passwords and to generate unique, hard to guess passwords for each site you use. Do not use the same password on more than one account. Each account should use a unique and strong password, at least 15 characters in length. A password manager will help keep track of passwords. And enabling the password manager's browser extension means you never have to type in passwords - the password manager does it for you. You can also use a password manager to share sensitive passwords with staff and vendors without directly exposing those passwords.

UPDATE SOFTWARE and APPS

Many software updates you see are for purposes of enhancing security or fixing security holes that could be exploited. So be sure to always install updates to your operating system, software, phones, and apps. Allowing software to auto-update is recommended.

SHARING FILES

Avoid sending attachments if possible. Instead, use a file sharing service like OneDrive or Google Drive to share documents. When a file is shared with you, don't click on the link in an email – instead log into the file sharing service and find the section to view files shared with you.

ENCRYPTED MESSAGING

When you have to share sensitive information, use an encrypted messaging app like Wickr or Signal. These guarantee both ends of the communication are secure and, unlike email or txt message, can't be easily hacked or intercepted. By default, Wickr doesn't keep messages longer than 30 days. With Signal, be sure to set it to keep no history of messages (you should enable "disappearing messages" for each conversation).

PHISHING EMAILS and TEXTS

Phishing attacks, in which an attacker attempts to trick you into giving them some information or clicking on a link to install malware, are becoming more and more common and now accounts for over 90% of successful hacks. Examples of phishing attacks are:

- Emails/Texts/DMs that appear to come from your bank, Google, or other institution that invite you to log into a fake website in order to steal your account credentials.
- Emails/Texts/DMs that appear to come from someone you know with a link or attachment containing malware. When you open the link or attachment, your computer is infected, and the attacker can gain access to content on your computer.

Be wary of any emails you are not expecting that contain links or attachments. Call the sender to confirm the email before opening any links or attachments. If you do have to click on a link (some services require you click on a link to confirm an account), before clicking hover your curser over the link to see the actual website it is sending you to - make sure it is what you are expecting (look for misspelled sites, example: goggle.com instead of google.com). Be particularly mindful of spear-phishing attacks – which are attacks using information specifically about you (or people you know) to construct a more plausible attack. **Clean up your "public" profile online**. Spear-phishing uses publicly available information from your Facebook, Twitter, or LinkedIn accounts. Adjust your privacy settings so only your friends can see information about you.

Authored by Ryan Borkenhagen
Rev 2.0, April 2019