DNC Information Security Checklist

Here is a checklist you can use to improve security of your devices and accounts. We recommend that you set aside time with your teams each month to print out and review this list, and to hold each other accountable. After all, an intrusion into someone else's account can lead to an intrusion in yours. We all need to find ways to protect the herd.

Secure Your Devices

When your phone or laptop has a software update, install it as soon as possible. Those updates will have important security improvements. Keeping your systems and apps patched is one of the most important ways to keep your data and accounts secure.

In the past 30 days I have:

- ❏ manually looked for and applied all operating system and application updates to my Mac
- ❏ manually looked for and applied all operating system updates to my PC
- ❏ manually looked for and applied all operating system updates to my iPhone/iPad
- ❏ manually looked for and applied all operating system updates to my Android phone
- ❏ manually looked for and applied all operating system updates to my Chromebook
- ❏ updated all my phone apps (iPhone, Android)
- ❏ updated all my laptop apps (Mac, Windows)

Encrypting your laptop can keep your data safe even when it's lost or stolen. All modern phones have encryption turned on by default, but you'll need to turn encryption on your computers. (instructions here: Macs, PCs) And use a strong **unlock code** on phones, and password/passphrase on laptops.

- ❏ My laptop drive is encrypted
- ❏ The passphrase on my laptop is longer than 12 characters long
- ❏ My phone has an unlock code that is at least 6 characters long

Secure Your Accounts

Practice strong password management. Use **long** (over 15 characters), **unique** (never used anywhere else) passwords. Long passwords make it hard for our adversaries to crack them. Unique passwords protect you when one site has a breach. Why? Because even if someone learns that one password, it will not work on any of your other accounts. Our adversaries count on you reusing passwords, so don't do it. You don't want an attack on one account to jeopardize any other accounts.

Some tips:

- Use a password generator to create a strong password, such as http://correcthorsebatterystaple.net/ or this passphrase generator
- How can you remember all these long, unique passwords? You can't. So use a password manager such as LastPass or 1Password to help create, store, and type them for you. That last

part is important. The password manager can insert your user name and password on the login page for you, meaning you never need to remember the password, or to copy/paste it.

Checklist:

- ❏ I use a password manager to store all my passwords
- ❏ The master password for my password manager is longer than 16 characters and is unique

Two-factor authentication (sometimes called 2FA, “multi-factor”, or MFA) will stop the most common phishing attacks against your personal and work accounts. Especially valuable to attackers are mail and social media accounts. Visit https://twofactorauth.org for instructions for popular sites.

Social media accounts include Twitter, Facebook, Instagram, Flickr
Email accounts include GMail, AppleID, Outlook365, live.com, Hotmail, Yahoo, AOL

In the past 30 days I have confirmed that:

- ❏ all my *personal* social media accounts require 2FA to login
- ❏ all my *work* social media accounts require 2FA to login
- ❏ all my *personal* email accounts require 2FA to login
- ❏ all my *work* email accounts require 2FA to login
- ❏ all my *personal* mobile devices require an additional security PIN if offered as an option
- ❏ all my *personal* banking accounts have long, unique passwords, and 2FA if offered as an option

Important note: Attackers will follow the path of least resistance. If you harden your personal and work accounts, the next best path may be through family members. Although we realize it may be a challenge to get families to complete this checklist, the reality of the current climate is that they should.