CYBERSECURITY
FOR STATE LEADERS

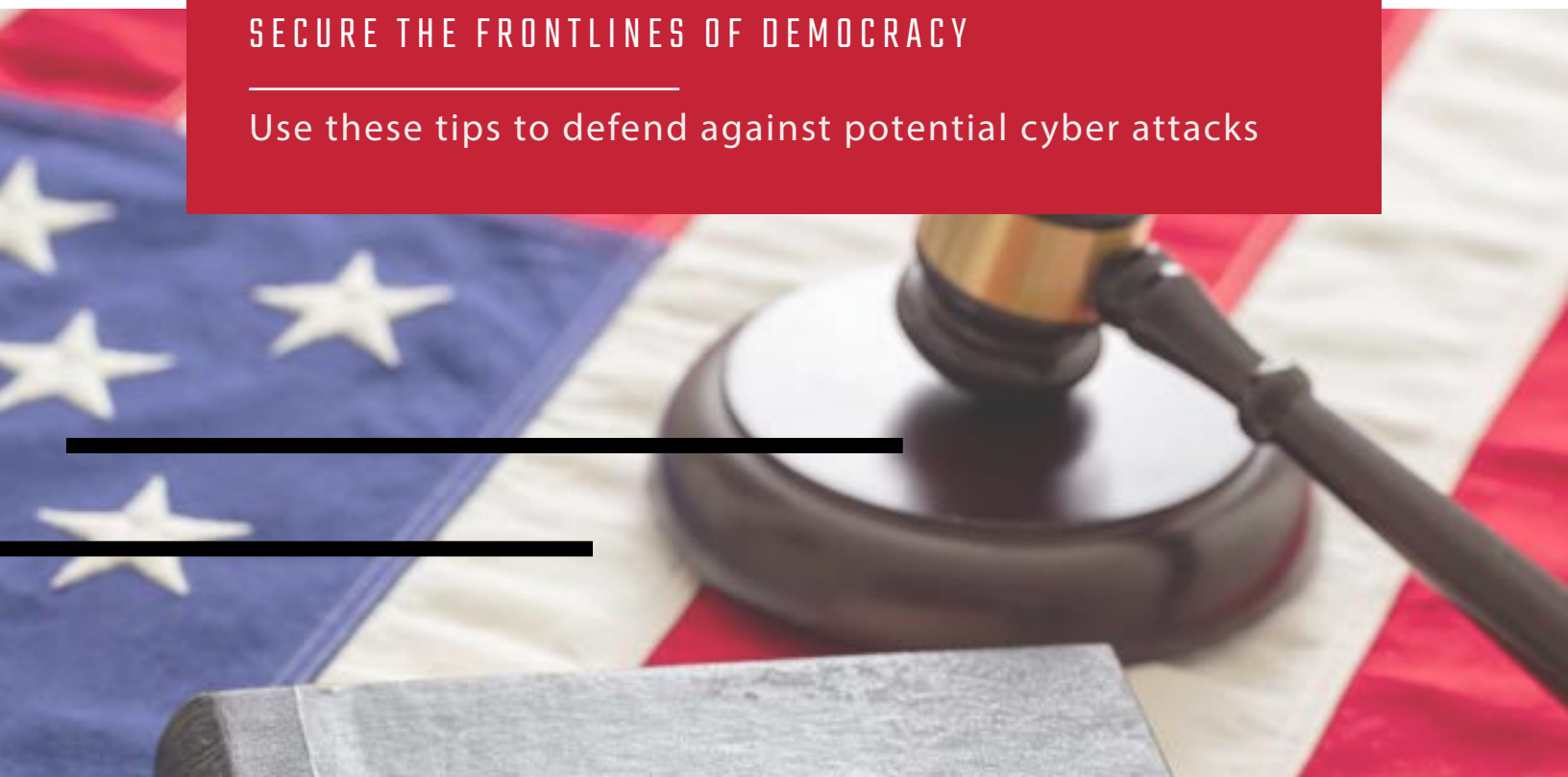
CYBERSECURITY GUIDEBOOK

CYBERSECURITY
GUIDEBOOK

YOUR GUIDEBOOK TO HELPING US

SECURE THE FRONTLINES OF DEMOCRACY

Use these tips to defend against potential cyber attacks



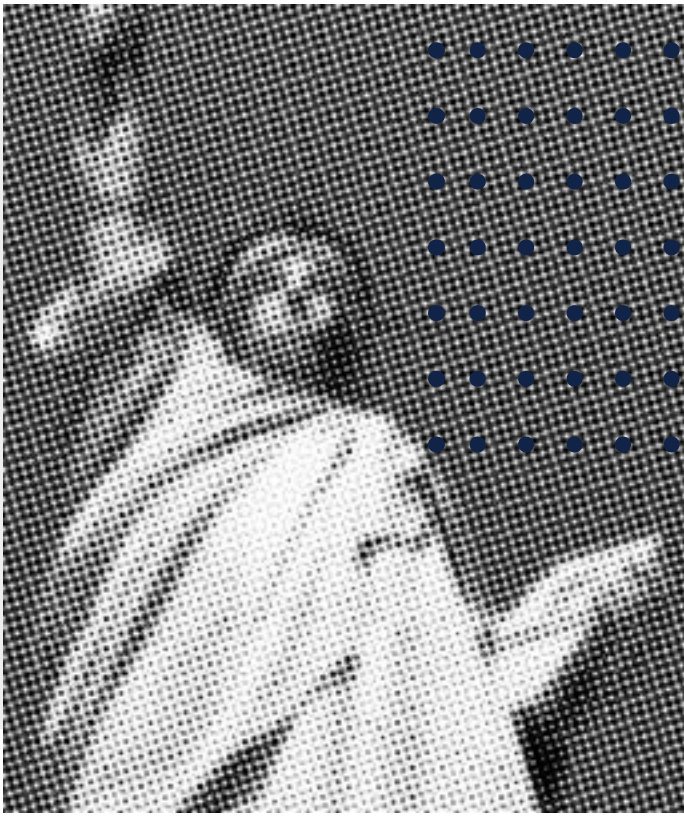
SECURING THE FRONTLINES OF DEMOCRACY

Our mission is to raise the level of cybersecurity awareness among state-level policy and decision makers so that they become an active part of defense for states by protecting fundamental government services that preserve democratic rights and values.

FIXING THE PROBLEM

CLOSING THE GAP

The National Cybersecurity Center (NCC), supported by Google, is launching a 50-state initiative to equip and empower state legislatures on cybersecurity best practices. This toolkit offers some easily implementable tactics on how to defend against typical attacks, but for a deeper dive be sure to sign up for the self-paced online modules at **cyberforstateleaders.org**.



TIP #1

DEPLOY MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication (MFA) is an authentication process that requires you to verify your identity through two or more methods to get access to things like an app on your phone or an online account. Usernames and passwords can be stolen or cracked, so MFA takes security to the next level by requiring additional sources of verification.

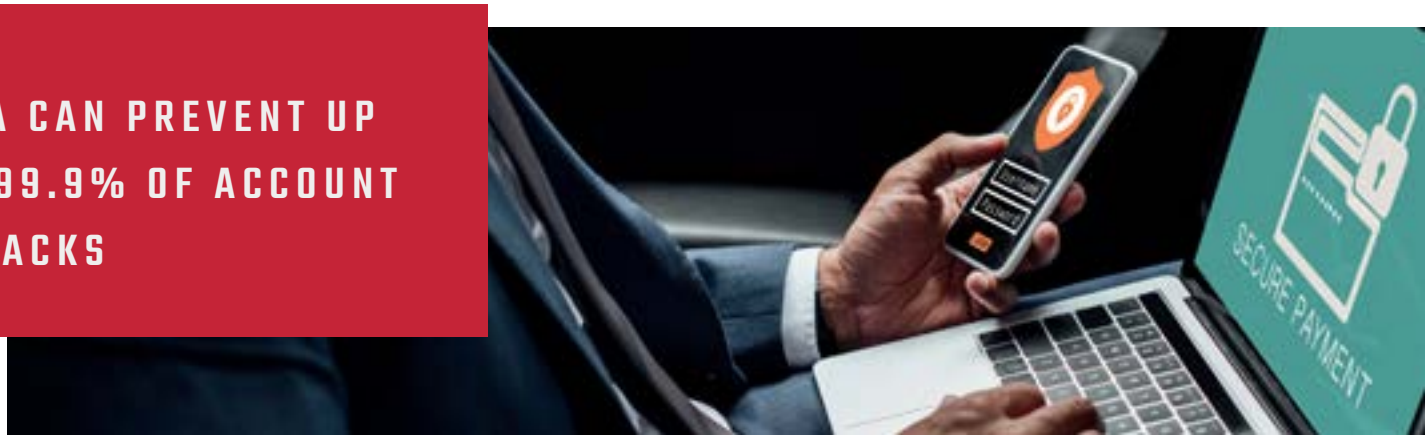
MFA verification relies on three different categories of information that are unique to you:

- What you know – like a password or a PIN
- Something you have – like a smartphone
- Something you are – like your fingerprint, face ID, or facial recognition

Some accounts make you sign up for MFA automatically. However, other accounts, like email accounts you have used for a while, may require you turn it on manually.

1. **Make a list of the accounts you use in which you may store personal or financial information.**
2. **Log into each account and find your "Settings" or "Account Information" tool, and select the security or privacy option – there should be a way to enable multi-factor authentication.**
3. **Turn on MFA and input the necessary information to complete the process.**
4. **If you're having trouble, try searching "how to enable multi-factor authentication on my ____ account". Most sites have developed a how-to!**

MFA CAN PREVENT UP TO 99.9% OF ACCOUNT ATTACKS



TIP #2

UPDATE SOFTWARE REGULARLY

Software updates replace old versions of software with newer versions that improve functionality and security. Examples of software include your web browser (Chrome, Microsoft Edge, Safari, Firefox), your Microsoft Suite products (Outlook, Excel, Word, PowerPoint), and other applications you use on your smartphone (or your smartphone's software itself).

Since attack methods are constantly evolving, software must also evolve to mitigate attacks. If we keep outdated software on our devices (i.e., your operating system), it's like leaving a window unlocked in our house just waiting for the right criminal to find it.

Most software will notify users of updates available, so keep an eye out for those notifications and accept them/install them as soon as possible Check with your IT provider/ department to ensure that these updates are legitmate.

1. **When you see a software update notification pop up on your computer or phone, don't close it!**
2. **Most software updates allow you to select a time that is most convenient for you to conduct the update. Choose a time when you don't need to be on your device to install the update.**
3. **Don't procrastinate. The longer you wait to allow a software update, the longer you're leaving that 'window' open for criminals to get into.**
4. **Automate updates when you can. There is often an option to "automatically update" your software which keeps you from having to think about it!**

TIP #3

STRONG PASSWORDS

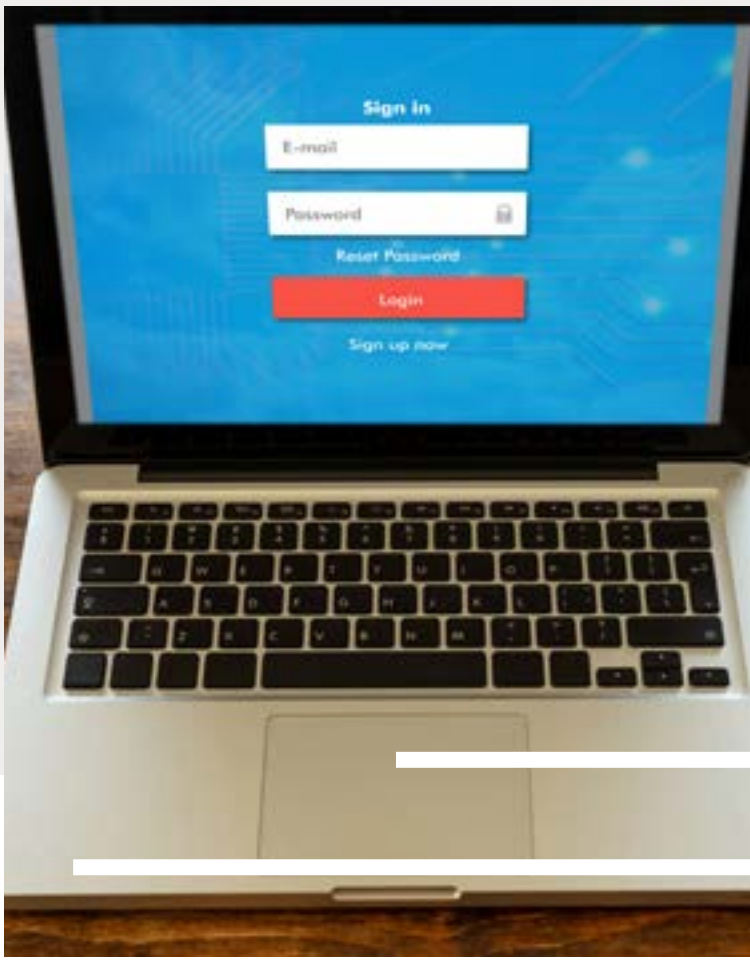
Strong passwords keep your accounts and information safe by making it harder for hackers. Without a strong password, criminals who spend days searching password dictionaries can easily unpack your password and your accounts.

1 **Avoid using the same password for multiple devices and accounts. A password manager can help manager this for you!**

2 **Short passphrases (even complicated ones) make it easier for hackers to identify. Use over 10 characters (including upper case, numbers, and characters like @#$%, for example).**

3 **Avoid personal information or common words. We put A LOT of information on the internet. We might be tagged in interviews that include personal anecdotes, or we answer social media surveys that share info such as where we went to high school or the year we graduated. All these pieces of information can add up to hints for hackers.**

4 **Deploy Multi-Factor Authentication! (Refer to the "Deploy Multi Factor Authentication" Section)**



TIP #4

ENCRYPT YOUR STUFF

When you encrypt a file or an email, you secure it by requiring a password (that you set) to open it. This extra step for your files or emails creates yet another layer of defense around sensitive materials.

Making sure that you back up your files goes together with encryption. Backups create copies of important documents that you don't want to lose in case something happens to your device.

When you send important information that might include your social security number, or details for a political campaign strategy, you can now rest a bit easier that it won't be opened by the wrong person. And if you regularly back up your important files, you can also relax knowing that you won't lose those critical campaign docs if you spill coffee on your laptop or flush your phone down the toilet.

Remember to check with your IT department or provider for organiztaional settings to determine when manual encryption of email is necessary.

TIPS FOR ENCRYPTING EMAIL IN MICROSOFT OUTLOOK

https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc

TIPS FOR ENCRYPTING EMAIL IN GOOGLE

https://support.google.com/mail/answer/6330403?hl=en

BACKUP YOUR STUFF

For backups, consider using an external hard drive to back up things that you don't need to regularly access, but want to keep. Complement the hard drive with cloud storage like Google Drive, Microsoft OneDrive, and iCloud. There are even programs that automate backups for you like Carbonite and Backblaze.

TIP #5

DON'T CLICK ON THINGS YOU SHOULDN'T
(AND WHAT TO DO IF YOU ACCIDENTALLY DID)

Hackers use tools that impersonate companies or people you know. They do this to trick you into purchasing something you don't need, or accidentally handing over personal information, financial information, or passwords.

Sometimes it's hard to tell what's real or not, so before you do anything:

STOP **Take a deep breath before you open that email or text. Does the email look familiar and accurate? Are there weird misspellings in the title?**

DON'T CLICK OR SHARE **Do your best to not click on any links in an email or a text from a source you aren't sure about.**

CONTACT YOUR IT RESOURCES **If you think you have received a suspicious email, report it right away as spam or junk and then contact your IT resource.**

If you did accidentally click on something that was suspicious:

- Don't enter any additional information
- Disconnect from the internet
- Scan your machine using an antivirus/antimalware software
- Change your passwords
- Contact your security team if it's an organization's resource (workstation or smartphone)
- Vist the FCC's website at https://www.identitytheft.gov/info-lost-or-stolen for tips on how to protect yourself if personal information was entereted

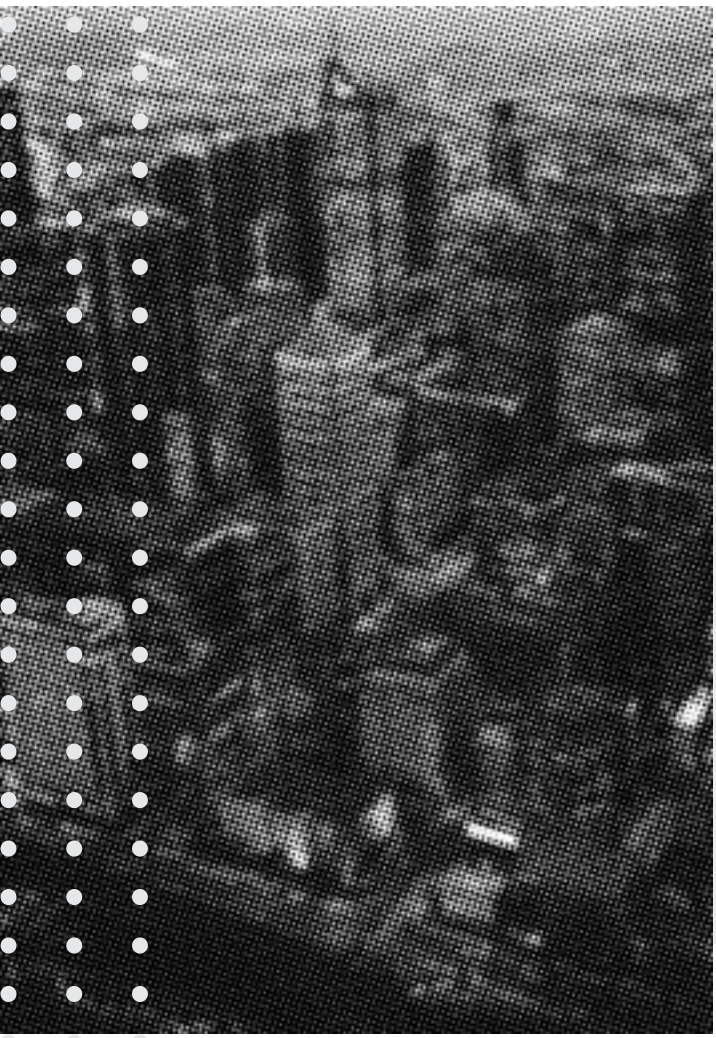
PREVENTATIVE CARE:
MAKE SURE YOU HAVE BACKED UP YOUR FILES AND TRY PROGRAMS LIKE GOOGLE'S PHISHING PROTECTION API.

TIP #6

SIM SWAPPING

Your phone's SIM card tells your phone which cell network to connect to and which phone number to use.

SIM swapping is what happens when a hacker calls your wireless carrier pretending to be you (using data usually available from previous hacks or breaches), and convinces them to assign your phone number to their SIM card. If successful, they get all of your text messages and calls, including those PINs from all of your accounts using MFA.



1 **Be careful to not give any information to Robocalls or 'phishy' text messages.**

2 **Add a PIN code or password to your wireless account. You can do this via most online accounts or you can call customer service.**

3 **If you lose service on your phone, call the customer service number IMMEDIATELY:**

- AT&T: 1-800-288-2020
- T-Mobile: 1-800-937-8997
- Verizon: 1-800-922-0204
- Make sure to contact your financial institutions quickly as well to make sure the hacker hasn't changed your passwords or lodged any transactions.

TIP #7

MISINFORMATION & DISINFORMATION

Misinformation and disinformation swirls around us on a daily basis on a variety of important topics and from a variety of domestic and foreign sources. Increasingly, we are seeing information shared from files and emails that have been hacked, which means there may be a significant lack of context for information shared, so stay alert.

TO PROTECT YOURSELF AND OTHERS FROM SPREADING INACCURATE INFORMATION, FOLLOW THESE TIPS:

1. **Check multiple reliable sources of information to see if a similar story is being reported.**
2. **Check sources cited in the article you are reviewing to confirm they are real and credible.**
3. **Read all the way through. It's easy for us to stop at headlines, but important for us to get the context of the whole article.**
4. **Be careful to not share information you haven't read, and done your due diligence on.**

TIP #8

WHEN PHYSICAL SECURITY AND CYBERSECURITY INTERSECT

The challenge with physical security is that sometimes those cybersecurity protections you have in place can be bypassed if an intruder has physical access to your device or systems.

1 **Consider using a second factor of authentication - like a security key. It works together with your strong password in case the strong password is somehow compromised through a data breach.**

2 **Consider having an automatic lock on your device. This can be a short as 5 minutes, so that way if an employee steps away from a device, the system locks without the employee having to do anything.**

3 **Many Mobile Devices have built in remote wiping or tracking features - this can be activated if a device is lost or stolen and will turn that device into a digital paper weight.**

SCENARIOS TO THINK THROUGH

To help put this into practice, here are a couple scenarios that can get you planning in the right direction:

- What would happen if you needed to evacuate your building and be out of your office in 60 seconds? What devices could you quickly lockdown and what devices would remain open and unlocked and potentially have access to?
- What would happen if an employee called you to say that their device had been stolen from their home office overnight? How would you be able to restrict access to the data that's on that device, or to help prevent that employee from impersonated online?