DON'T GET

CYBERSECURITY FOR STATE LEADERS

DEPLOY MULTI-FACTOR AUTHENTICATION (MFA)

WHAT IS IT?

MFA is an authentication process requiring two or more methods in order to get access to things like an app on your phone or an online account.

MFA makes it harder for criminals to hack your passwords, and therefore your accounts.

HOW DOES IT WORK?

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

1. **What you know —** like a password or a PIN
2. **Something you have —** like a smartphone
3. **Something you are —** like your fingerprint, face ID, or voice recognition

SET IT UP

More online accounts and applications are moving to MFA for security. Some accounts and applications automatically require that you add another verification method when you sign up for an account or download an app.

If it isn't automatic, go to your settings + account (or security) to find the option.

UPDATE YOUR SOFTWARE REGULARLY

WHAT IS IT?

Software updates replace old versions of software with newer versions that improve functionality, and most importantly, security. Examples include your web browser (e.g. Chrome, Internet Explorer, Safari, Firefox), your Microsoft Suite products (e.g. Outlook, Excel, Word, PowerPoint), and other applications you use on your smartphone.

WHY DOES IT MATTER?

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 If we keep outdated software on our devices, it's like leaving a window unlocked in our house – just waiting for the right criminal to find it.

HOW DOES IT WORK?

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.

Where you can, choose to make software updates automatic.

PASSWORDS—MAKE THEM STRONG

WHY DOES IT MATTER?

Without a strong password, criminals who spend days searching password dictionaries can easily unpack your password, and therefore your accounts.

HOW TO MAKE THEM STRONG

1. **Make passwords unique –** avoid using the same password for multiple devices and accounts (password managers help with this!)
2. **Make them longer –** short passwords, even if they are complicated, still make it easier for hackers to identify. Use between 9-12 characters (upper and lower case letters, numbers and symbols), and you have a better chance at stumping them.
3. **Avoid personal information or common words –** We put A LOT of information on the internet these days, so avoid using words or phrases that could be traced back by someone with some basic observation skills.

ENCRYPT AND BACKUP YOUR STUFF

WHAT DOES IT MEAN?

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.

WHY DOES IT MATTER?

Encryption makes sure that only the right person opens your email or documents.

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.

HOW DOES IT WORK?

Tips for encrypting email in Google - https://support.google.com/mail/answer/6330403?hl=en
Tips for encrypting email in Microsoft Outlook - https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc
Tips for backing up your important files -
Back up with multiple methods – 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.

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

WHAT DOES IT MEAN?

Hackers impersonate companies or people you may know to try to trick you into purchasing something you don't need to, handing over personal and financial information, or your passwords.

WHY DOES IT MATTER?

Nearly one-third of all data breaches in the U.S. last year were the result of people clicking on links from malicious actors or sharing password information. That's a pretty big deal. Just think, if someone hadn't clicked the link, or shared the password. That means money saved data saved, and a whole lot less headaches.

HOW TO TELL?

Sometimes it's hard to tell what's real or not. If you get something suspicious: **Stop, don't click or share, and contact your IT resource.**

If you accidentally do click on something you shouldn't:

- Stop here – don't enter any additional information
- Disconnect from the internet
- Scan your machine using anti-virus/antimalware software
- Change passwords to accounts with your personal or financial information
- Try programs like Google's Phishing Protection API - https://cloud.google.com/phishing-protec-tion/docs/quick-startsubmission-api