



Cyber Security

Tips to help keep YOUR Data Safe

AFSCME Code of Conduct

- AFSCME is committed to providing an environment free from discrimination and harassment, regardless of an individual's race, ethnicity, religion, color, sex, age, national origin, sexual orientation, disability, gender identity or expression, ancestry, pregnancy, or any other characteristics prohibited by law. As such, AFSCME will not tolerate discriminatory, harassing or otherwise unacceptable behavior at any of its activities, events or meetings. AFSCME expects everyone who participates in any of its activities, events or meetings to abide by this standard of conduct.
- There will be no retaliation or other adverse action taken against an individual who makes a complaint. Complaints should be sent to the AFSCME Human Resources Department at reportharassment@afscme.org



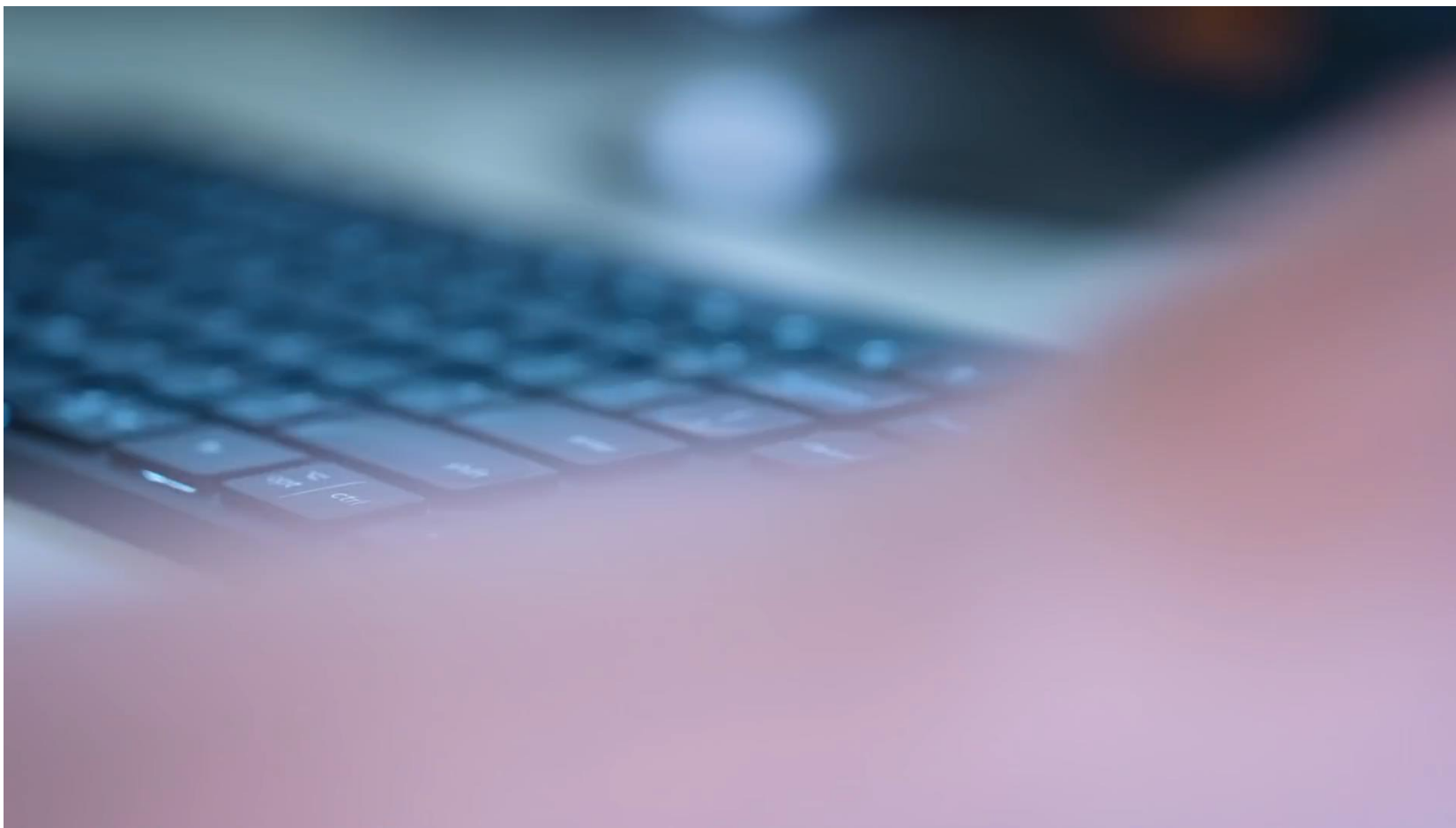
Objectives

- Create awareness of Information Technology (IT) threats.
- Explain the responsibility of the user.
- Encourage appropriate responses to threats and infections.
- Inform your staff about your IT Policy and procedures.

What if we were talking IRL not via technology?



How Much of a Threat is Ransomware??



Why We Don't Want Users Opening Links or Attachments from UNKNOWN Senders.



Where does cybersecurity start?

- Report problems as soon as possible
- Defend your computer
- Protect your data
- Create strong passwords and keep them private
- Guard data when you're on the go



Reporting Problems

If you lose your laptop, smartphone, or other device, or sensitive data or accounts have been compromised by theft or a breach of internet/network security:

1. Report it immediately to your IT professional, your manager, and your provider when appropriate.
2. Change all passwords used to log on to the device.
3. Contact IT for help in wiping the data from smartphones and securing other devices.



Reporting Problems

- Infection of Malware, Virus, Ransomware, or unknown infection
- Contact IT immediately whether device is in the building, the road or at your home.



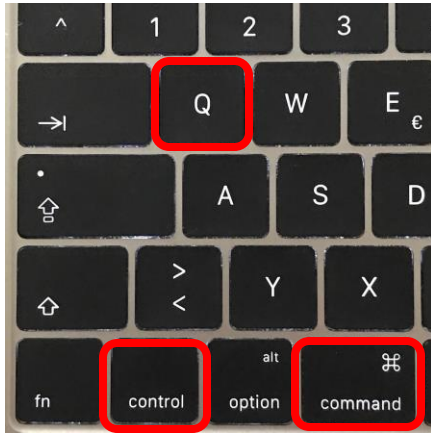
[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Reporting Problems

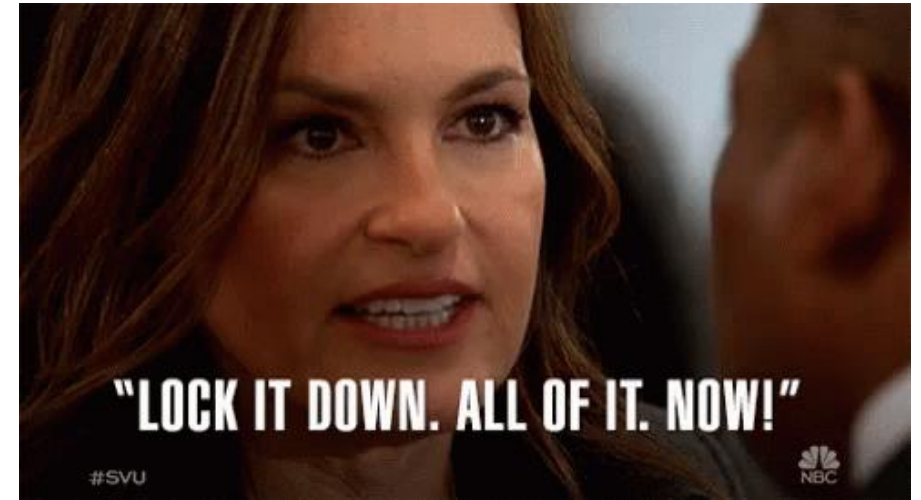


- When in doubt: **Report**
- Not sure if your computer, email, or data is affected also report it immediately.

Defend Your Computer By: Locking your Computer When You Walk Away



Control +
Command + Q:
Immediately lock
your screen.

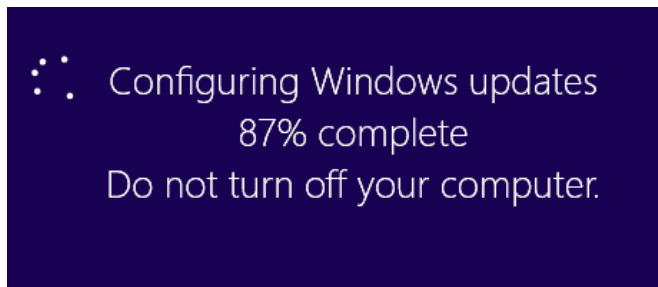


Windows logo key + L: Lock your PC

Defend your computers – Virus Protection



Defend your computers– Latest OS



Don't Be Fooled Into Downloading Malicious Software

- Remind users to beware of suspicious emails/links.
- Everyone should ask an IT professional before installing software of any type especially from the web.



Protect Member Data

- Don't put confidential information in:
 - email, instant messages, or text messages they may not be secure.
- Contact your IT Dept. if you need secure options.
- Don't send staff email to their personal email address (be careful with individuals you know personally and in workplace. AFSCME member DATA should never go to personal account.)
- Beware of scams. Never give information like an account number or password in response to a phone call, or email or another online request.
- Avoid the risks and dangers of downloading free apps and games from the web.

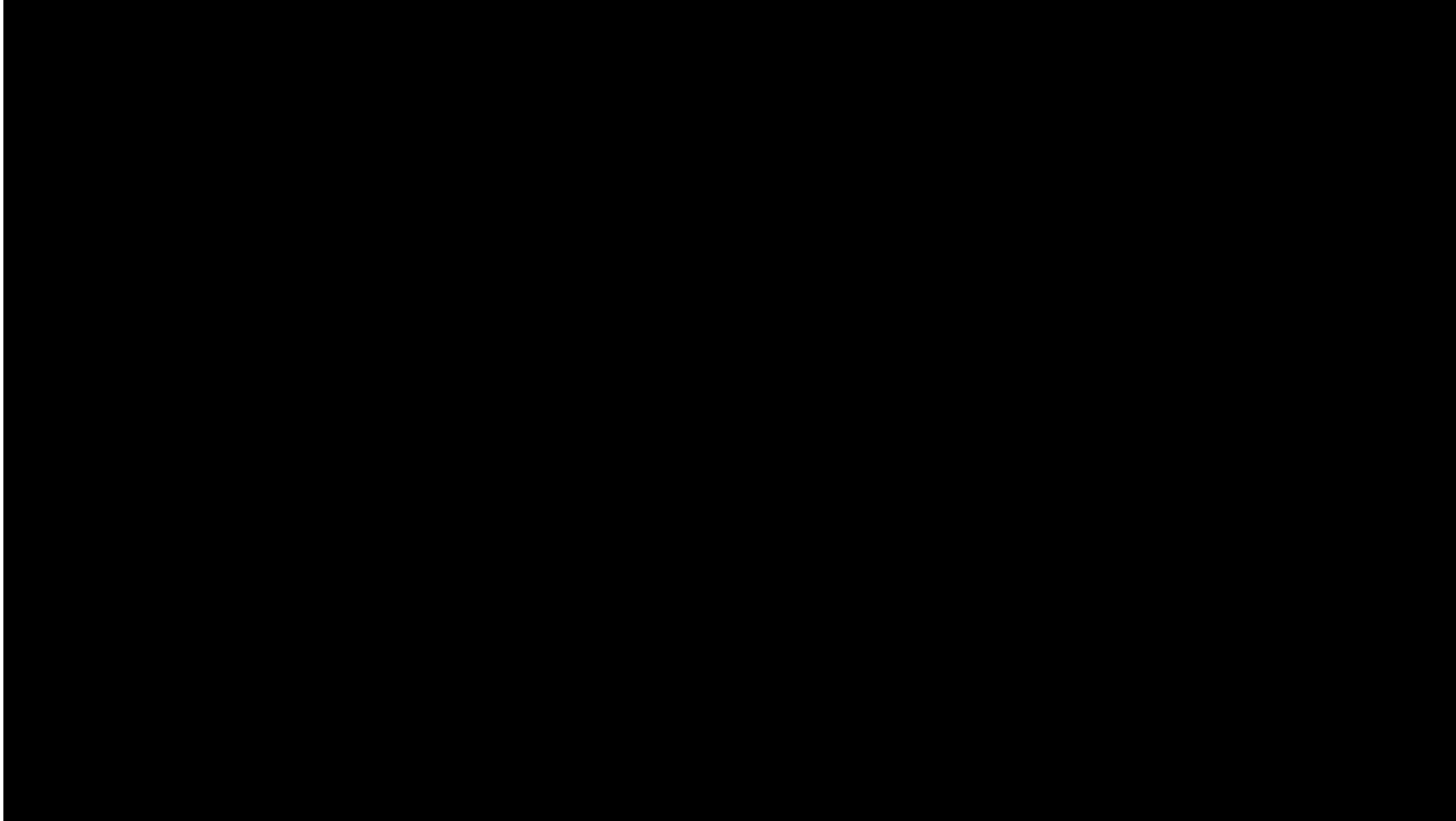




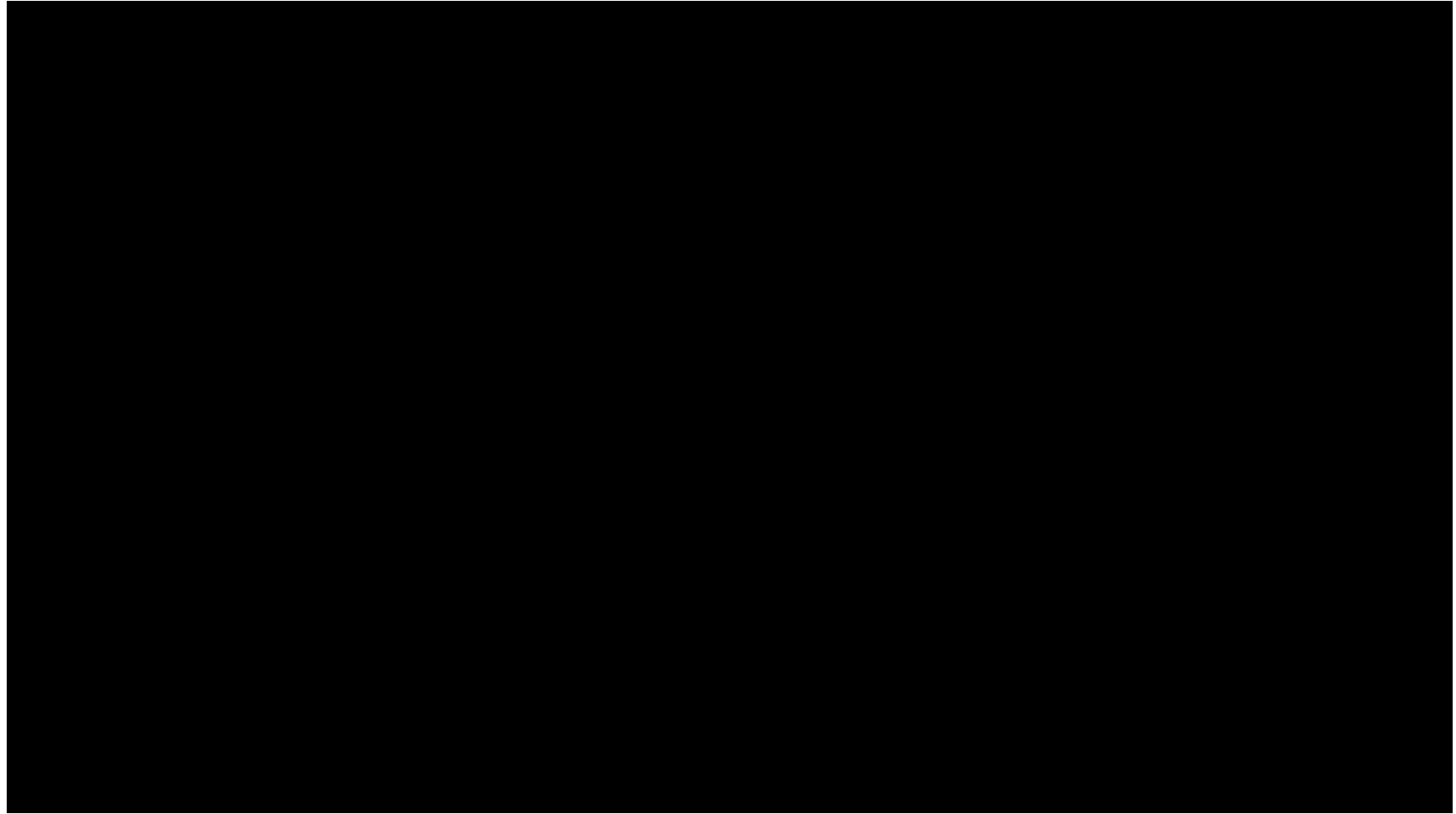
What is Phishing?



What about Vishing? – Voice Phishing



Smishing? WHAT THE PH?



Phishing

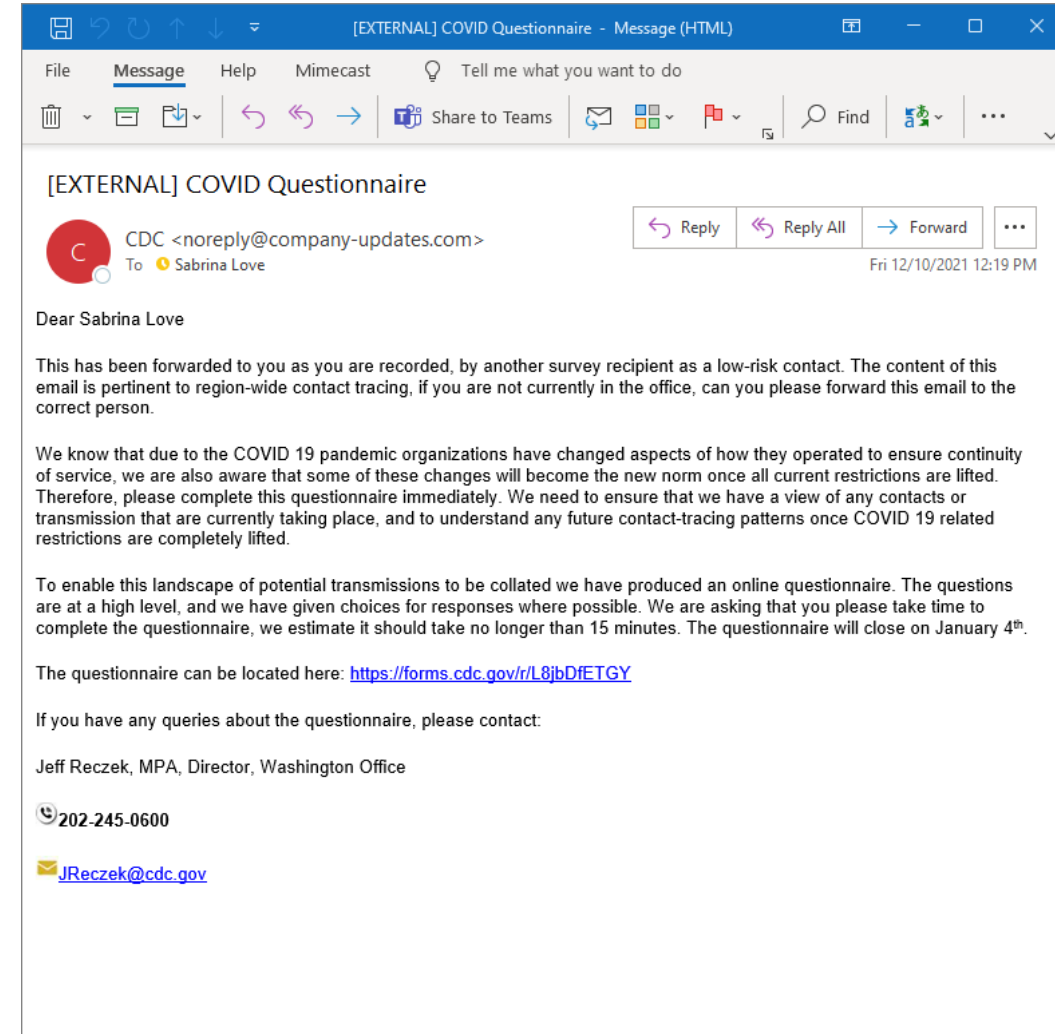
- Most frequent attack that we experience at AFSCME IU.
- Conduct phishing exercises.
- Identify where to send any suspicious emails.



Example of Phishing Exercise

Things to look out for:

- From address:
 - Do you know the person emailing?
 - Is this the CDC website?
- Does this make sense:
 - Before clicking on the email or sending to someone else carefully read it.
 - How should you act on it?



Create Strong Passwords and Keep Them Private

- Use a unique password
- Making a complex password
- Same password for multiple accounts makes them all vulnerable

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



> Learn about our methodology at hivesystems.io/password



What Happens If Your Password Is Stolen or Given Away!!

- It doesn't matter how complicated your password is if it is compromised.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

Create strong passwords and keep them private

Do

Do make the new password significantly different from previous passwords.

Do use a sentence or phrase converted into a string of initials, numbers, and symbols.

Do make your password hard to guess even if someone knows a lot about you (avoid names and birthdays of your family or your favorite band).

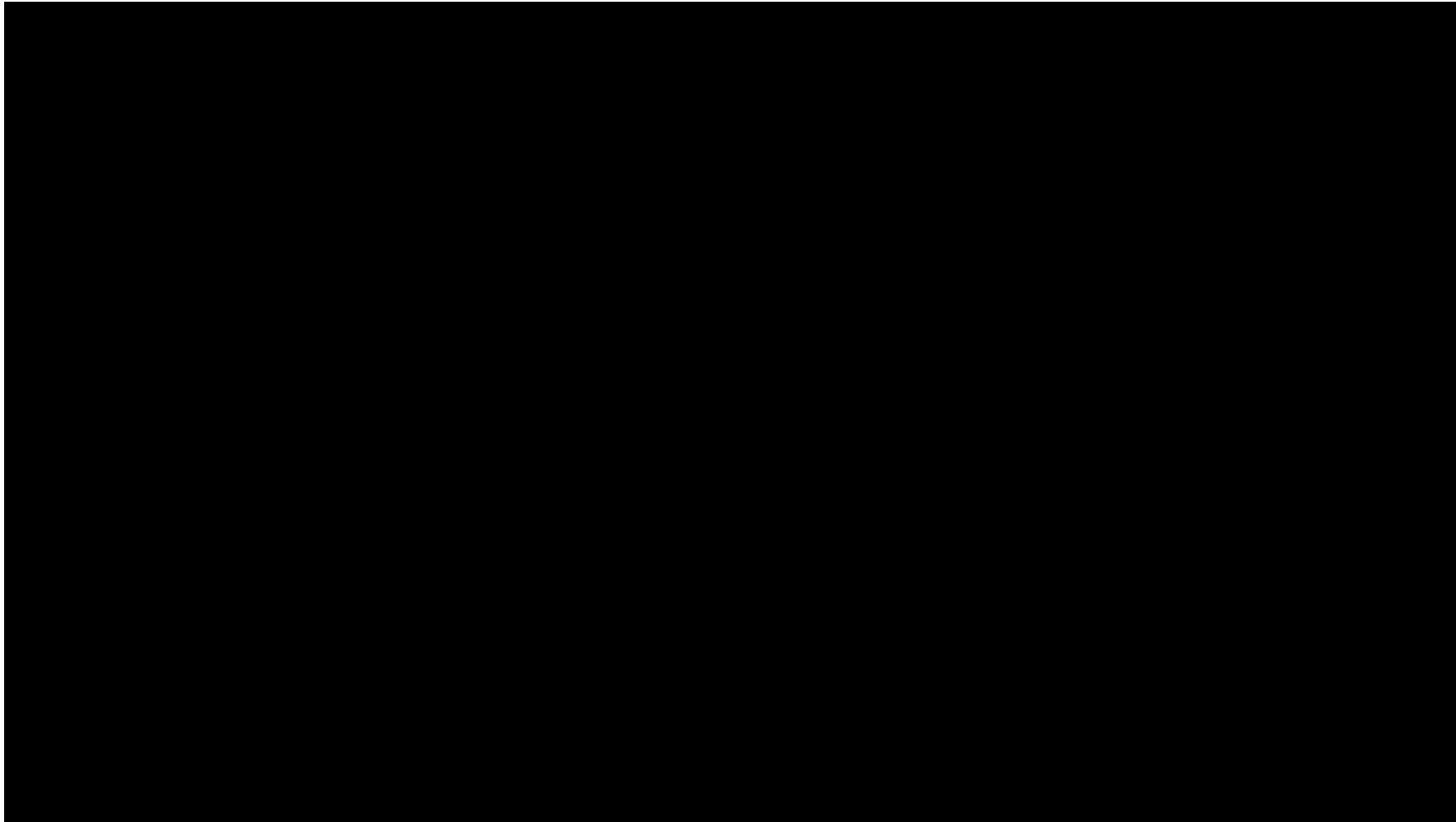
Don't

Don't use the same password for different accounts.

Don't use a single word for your password like "afscme," "money," or "sunshine."

Don't use common passwords like "password," "iloveyou," or "12345678."

Multi-Factor Authentication



Guard Data When You're on the Go - Wi-Fi

Treat all Wi-Fi networks you don't control as a security risk.

- Verify the network
 - Use your own hotspot
- Avoid sensitive data
- Turn off Wi-Fi when down

Questions?

Guard Data When You're on the Go

– Flash Drives

- Do not use flash drives unless there is no other option. Minimize the chance that you'll infect your computer & your network with malware.

