

# 31 DAYS OF CYBERSECURITY AWARENESS

It's up to each of us as individuals, and collectively, as a society, to protect our personal and business information online, and make the Internet a safer place. Our workplaces, homes, schools, and other public spaces are Internet-connected and vulnerable. We all need to take steps to ensure our cybersecurity.

*These tips are designed to help everyone learn more about cybersecurity and create habits to protect ourselves, our organizations and our customers.*

01

## YOU ARE NOT IMMUNE

Get out of the mindset that an attack can't happen to you.

## DON'T "SEE ATTACHED" IN EMAILS

Don't open email attachments you weren't expecting to receive.

02

## AUDIT YOUR PASSWORDS

Make sure they contain an assortment of characters and change them regularly.

03

## CONNECT SECURELY

Don't use unsecured or public Wi-Fi networks to conduct business.

05

## PATCH REGULARLY

Update software on your devices and systems on a regular basis to fix bugs and performance issues.

08

## TAKE A PHISHING QUIZ

Test your ability to spot the differences between real emails and phishing emails.

07

## ASSESS YOUR RISKS

Understand what threats you or your organization may be vulnerable to and fix them.

06

## UPDATE YOUR BROWSERS

Make sure you're using the latest versions of your Internet browsers and any related plugins.

09

## TRUST NO ONE ON SOCIAL MEDIA

Take a closer look at your social media connections and don't accept invites from people you don't know.

10

## USE STRONG PASSWORDS

Lock your phone, computer and other devices with a secure passcode.

11

## VALIDATE, THEN INSTALL

Carefully vet antivirus, firewall and ad-blocker solutions.

12

## MULTI-FACTOR AUTHENTICATION

Apply additional security measures to your accounts to better protect them.

13

## CONDUCT REGULAR PENTESTS

Assess the effectiveness of security controls and policies with an annual or more frequent test.

16

## DISABLE AUTO-CONNECT

Make sure your Wi-Fi auto-discovery function and Bluetooth is off when you're traveling or in public.

15

## CONTROL APP ACCESS

Get into the habit of not installing any apps unless they come from the official app store.

14

## CLEAN UP YOUR APPS

Remove any apps you're not using and updating frequently.

17

## HELP OTHERS STAY SECURE

Share your security knowledge and resources with anyone who could use the guidance.

18

## MIND YOUR SURROUNDINGS

Before you use a USB you found or answer a request for a software update, ask questions, do your own independent research and don't be afraid to say no.

19

## UPDATE YOUR SOFTWARE

Make sure any software you use on your computer is updated regularly.

20

## BACK UP YOUR DATA

Back up your information frequently to protect critical data in case of a ransomware attack or system failure.

21

## MONITOR YOUR SYSTEMS

Continuously monitor your systems and applications to prevent security incidents.

24

## KEEP BACK UP INFORMATION CURRENT

Check and update the recovery email addresses, phone numbers and physical addresses associated with your accounts.

23

## DON'T CLICK LINKS FROM SUSPICIOUS SOURCES

Avoid clicking links from unknown or questionable sources.

22

## MONITOR ACCOUNT ACTIVITY

Track the activity logs for your accounts on a regular basis.

25

## PROTECT YOUR ENDPOINTS

Install antivirus on personal devices and next-gen Endpoint Detection and Response (EDR) on corporate assets.

26

## CREATE AN ALTERNATE EMAIL ADDRESS

Instead of using your primary email address for every online account, create an alternate email address for public-facing accounts and uses.

27

## STAY AWARE OF SCAMS

Pause before you share your information with anyone offering you something.

28

## DON'T GIVE AWAY ADMIN RIGHTS

If new software or a new app is asking for admin rights, find out if the access is required and why before approving it.

31

## CREATE A SECURITY PLAN

Develop a checklist for yourself and your organization and test it at least annually.

30

## THINK TWICE

Be sure you trust the source when opening attachments or files downloaded from the Internet.

29

## DISABLE LOCATION TRACKING

Turn off location tracking on apps and devices if they're not needed or you're not actively using them.

For more information on our full range of Cybersecurity Services, contact your Motorola Solutions representative or visit us at [www.motorolasolutions.com/cybersecurity](http://www.motorolasolutions.com/cybersecurity)

 **MOTOROLA SOLUTIONS**

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved. 09-2020

### Sources

Google Support  
<https://support.google.com/accounts/answer/32040>

SANS  
[https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602\\_en.pdf](https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_en.pdf)

National Cyber Security Alliance  
<https://staysafeonline.org/>

Norton  
<https://us.norton.com/internetsecurity-mobile-8-cyber-security-tips-for-business-travelers.html>

Mozilla  
<https://www.mozilla.org/en-US/teach/smarton/security/>