

Digital

SECURITY

1

Keep software up-to-date

- THIS INVOLVES VERIFYING THE IDENTITY OF USERS BEFORE GRANTING ACCESS TO DIGITAL RESOURCES. COMMON METHODS INCLUDE:**
- **PASSWORDS AND PINS (THOUGH THESE ARE OFTEN CONSIDERED INSUFFICIENT ON THEIR OWN).**
 - **MULTI-FACTOR AUTHENTICATION (MFA): REQUIRES MULTIPLE FORMS OF VERIFICATION, SUCH AS PASSWORDS AND ONE-TIME CODES SENT VIA SMS OR GENERATED BY AN APP.**
 - **BIOMETRIC AUTHENTICATION (E.G., FINGERPRINT, FACE RECOGNITION).**

2

AUTHENTICATION AND ACCESS CONTROL:

- **AUTHENTICATING THE IDENTITY OF A USER, SYSTEM, OR ENTITY BEFORE GRANTING ACCESS TO RESOURCES. IT ENSURES THAT THE PERSON OR SYSTEM REQUESTING ACCESS IS WHO THEY CLAIM TO BE.**
- **ACCESS CONTROL REFERS TO THE PROCEDURES AND GUIDELINES THAT ESTABLISH WHO HAS ACCESS TO WHAT RESOURCES AND UNDER WHAT CIRCUMSTANCES. IT MAKES ENSURING THAT SYSTEMS AND PEOPLE MAY ONLY ACCESS DATA AND TAKE ACTIVITIES THAT ARE PERMITTED TO THEM.**

KEEP HARDWARE UP-TO-DATE

3

THE LATEST SOFTWARE SECURITY UPDATES MIGHT NOT BE SUPPORTED BY OUTDATED COMPUTER HARDWARE. FURTHERMORE, OUTDATED GEAR SLOWS DOWN THE RESPONSE TO POTENTIAL CYBERATTACKS. USE MORE RECENT COMPUTER HARDWARE WHENEVER POSSIBLE.

USE ANTI-VIRUS AND ANTI-MALWARE

4

HAVING COMPLETE AND ABSOLUTE PROTECTION FROM MALWARE IS UNATTAINABLE AS LONG AS YOU REMAIN ONLINE. HOWEVER, BY MAKING SURE YOUR PCS HAVE AT LEAST ONE ANTI-MALWARE PROGRAM AND AN ANTIVIRUS PROGRAM INSTALLED, YOU MAY DRASTICALLY LOWER YOUR SUSCEPTIBILITY.

5

CHECK LINKS BEFORE YOU CLICK

IT'S ADVISABLE TO VERIFY BEFORE CLICKING ON A HYPERLINK BECAUSE THEY MIGHT BE READILY MISREPRESENTED. HOVERING OVER THE LINK IN THE MAJORITY OF BROWSERS WILL DISPLAY THE TARGET URL. TO VERIFY LINKS BEFORE CLICKING ON THEM, DO THIS.

