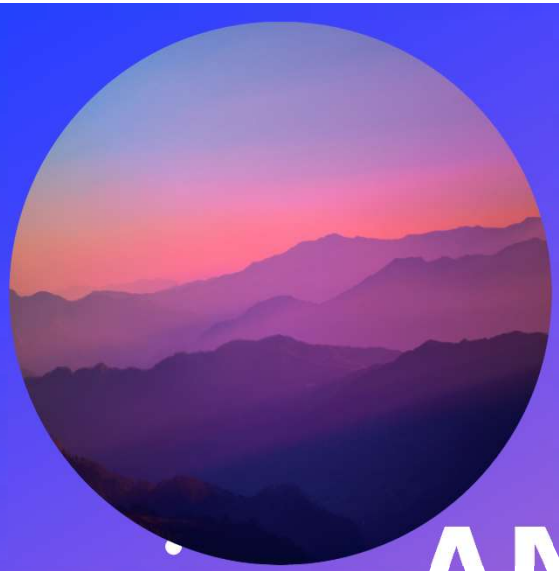
MINNESOTA TECH FOR SUCCESS

Week 11-12: IT Security

2/14/2024

Agenda

- **Announcements**
- **Classroom (25 min)**
  Steps to keep data secure
  Basics of encryption
- **Break (5 min)**
- **Warehouse (1.5 hrs)**
  Assemble g-Force HPs
  RAMs
  HDDs & SSD



ANNOUNCEMENTS

Week 12

Announcements for 2/14

- **Calendar**
  - Current Session – Week 12
  - Next session: **Wednesday, 2/21/2024**
- Week 11-12: IT Security – Feb. 7th & 14th
- Weeks 13-15: Cloud Computing – Feb 21st , 28th , & Mar 6th

Values

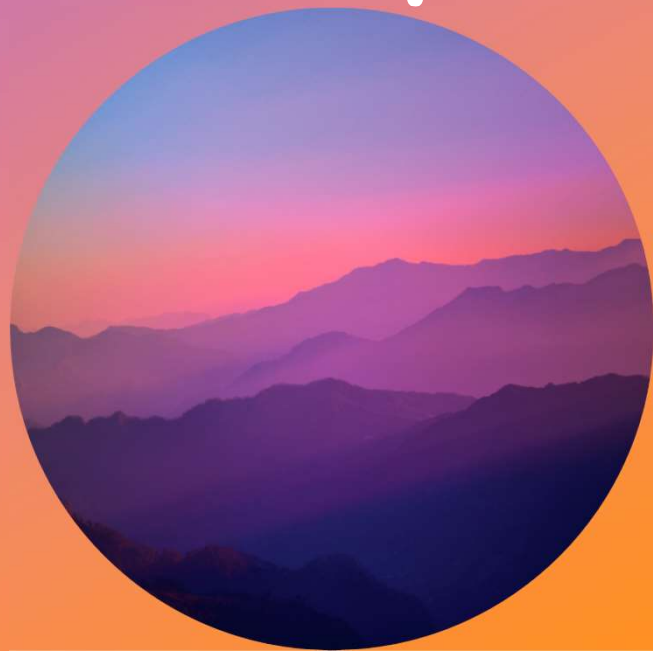
- **R**espect
- **A**ccountability
- **I**mprovement
- **S**teadfast
- **E**ncouragement

IT Security Objectives:

- Why IT security is important
  - Discussion on the significance of IT security in protecting data and privacy
- Everyday security threats
  - Identification of common security threats such as viruses, malware, and phishing
- Simple steps to keep data secure
  - Introduction to basic security practices, including password management and data backup
- Basics of encryption
  - An overview of encryption and its role in securing data during transmission and storage

IT SECURITY

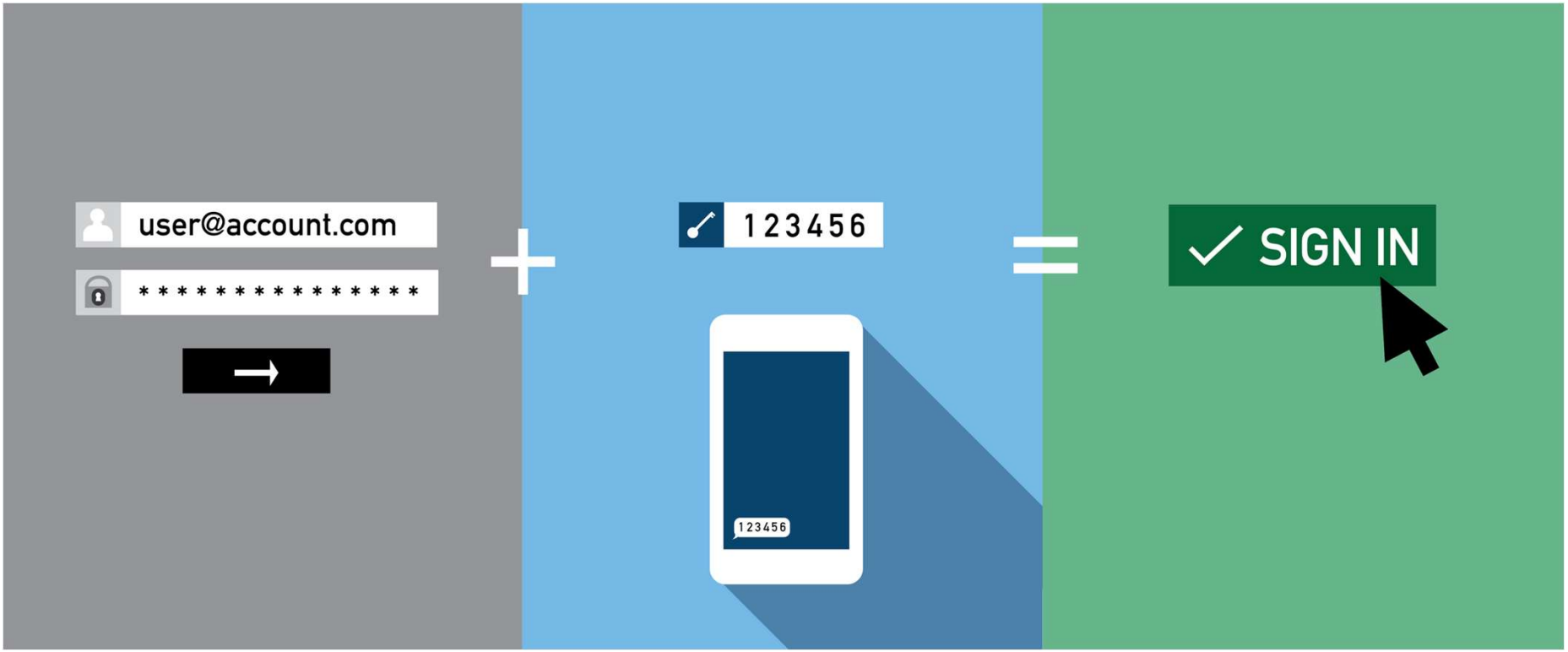
Steps to keep data secure



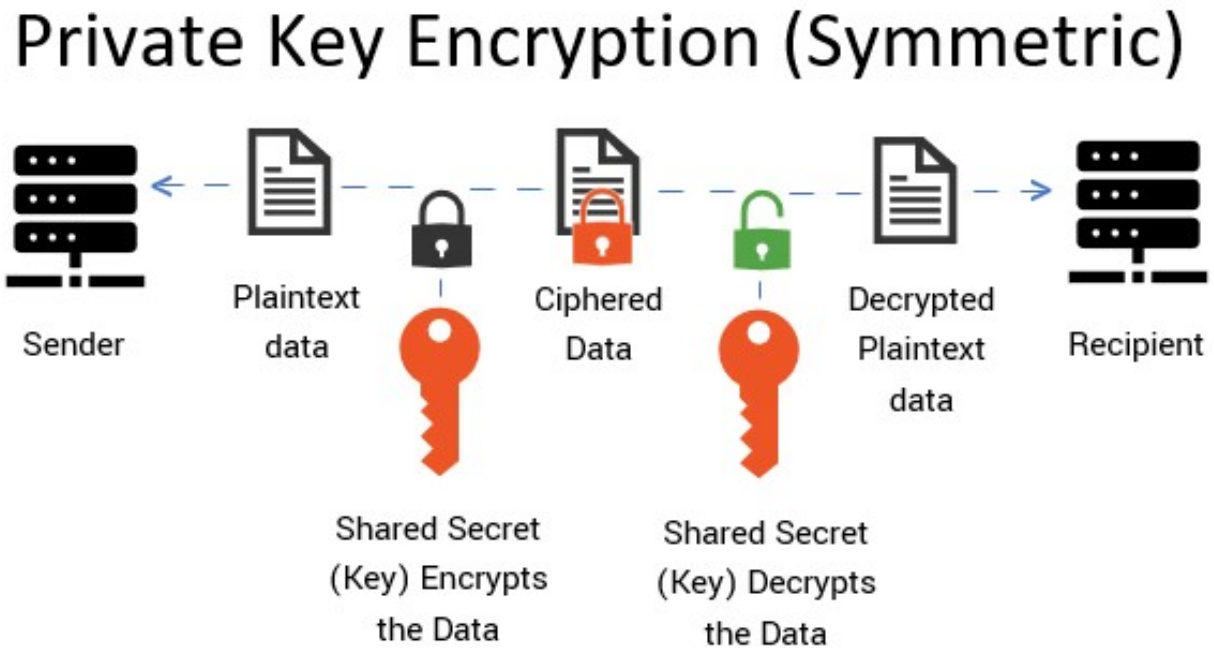
Data Security: Definitions

- Multifactor authentication (MFA) – protects applications or online accounts by using one or more sources of validation/verification factors before granting access to the user
- Public Key Infrastructure (PKI) – roles, policies, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption
- Encryption– cybersecurity measure that scrambles plain text, so it can only be read by the user who has the secret code or decryption key
- Encryption key – series of numbers which are created with algorithms (random and unique) that encrypt and decrypt data
  - Symmetric encryption – same key used for both encryption & decryption
  - Asymmetric encryption – two different keys are used: public key, private key
- Digital Signature – numeric string that verifies the authenticity and integrity of digital data which validates the identity of the sender and protects the data from unauthorized modifications
- Digital Certificate – a document that is issued by a trusted Certificate Authority (CA) which binds an entity's identity to a public key and facilitates secure communication

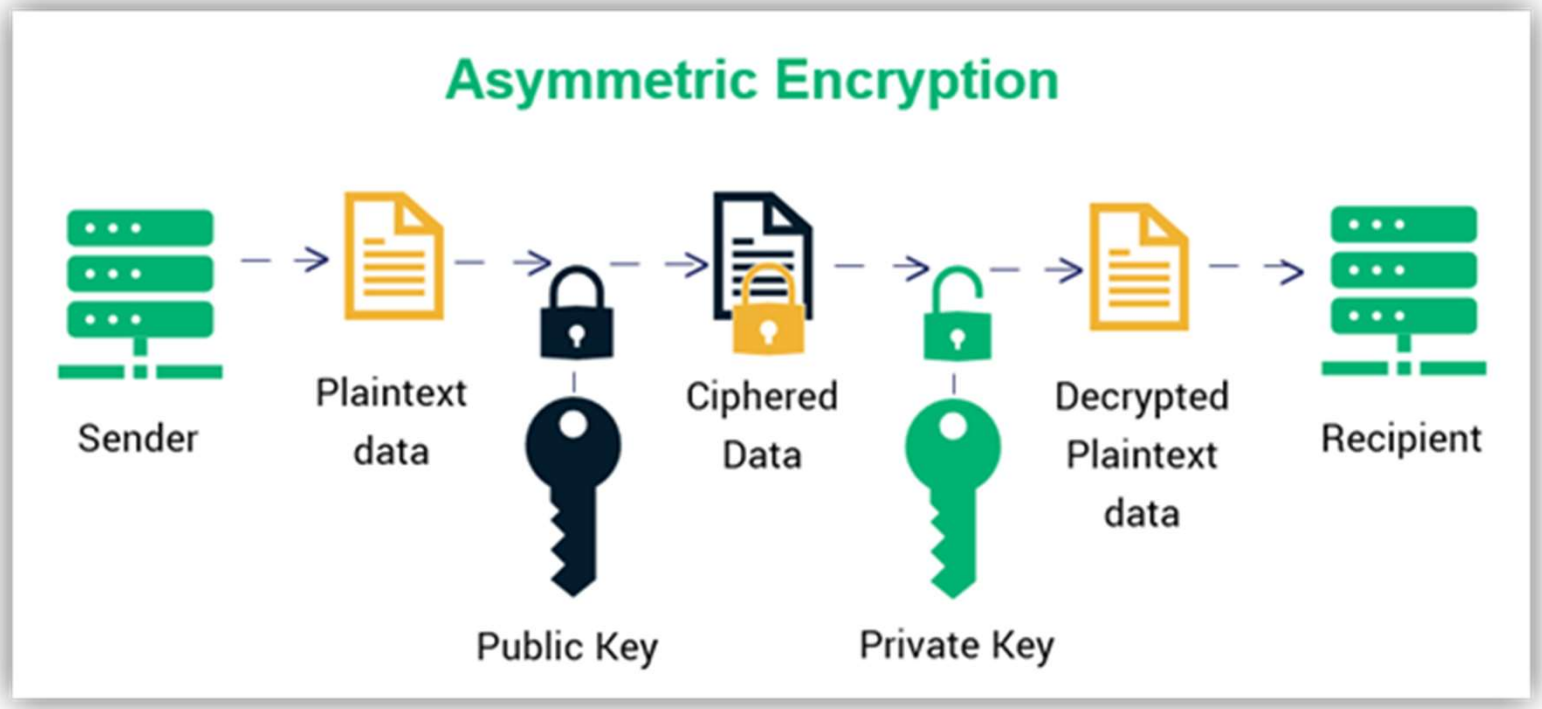
MFA



PKI


Private Key Encryption (Symmetric)
Sender
Plaintext data
Shared Secret (Key) Encrypts the Data
Ciphered Data
Shared Secret (Key) Decrypts the Data
Decrypted Plaintext data
Recipient

PKI


Asymmetric Encryption
Sender
Plaintext data
Public Key
Ciphered Data
Private Key
Decrypted Plaintext data
Recipient

Data Security: Ways to Secure Data

- Lock computer while away from it: **[WIN] + [L]**
- Back up regularly to avoid data loss (causes due to cyberattacks, natural disasters, human errors etc.)
- Keep software up to date
  - New updates to bug fixes and patch security vulnerabilities
- Follow password protection standards
  - Compliance Standards – EU General Data Protection Regulation (GDPR)
- Use a VPN to create an encrypted tunnel for data
- Use antivirus software
- Set up and use multifactor authentication (MFA)
- Utilize a public key infrastructure (PKI)
- Enable Location Services on device when not using VPN
- Educate yourself and others on cybersecurity best practices & policies

Data Security: Password Management

- Create a strong, long passphrase (6 or more characters long; special characters)
- Use different passwords for every account
- Secure smartphone/personal computer
- **Avoid:** using dictionary words, PII (personally Identifiable information), reusing passwords, saving autofill passwords to the browser
- Optional: Store and/or use autogenerated passwords from a Password Manager (i.e. bitwarden, LastPass)

Data Security: Data Backup

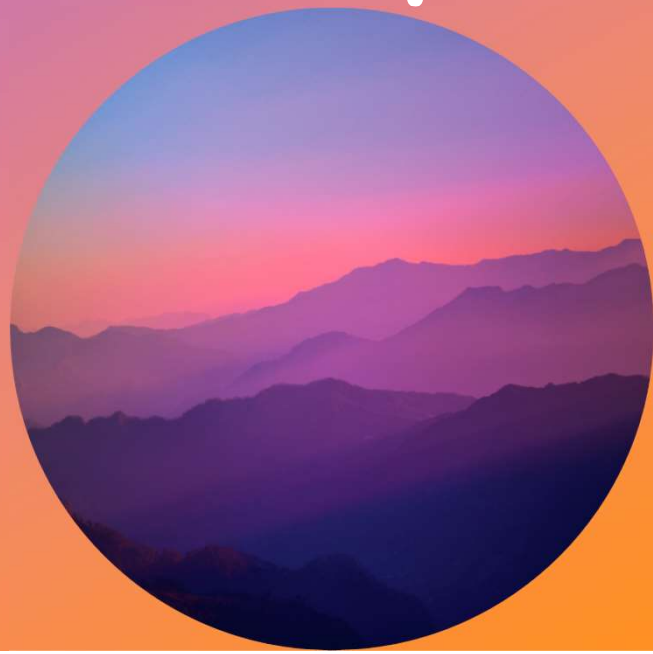
- Cloud Storage
  - iCloud, Google Drive, OneDrive, Dropbox, Azure Disk Storage
  - Pros: Secured remote location, free & low-cost upgrades, access it anywhere with internet, managed by the host
  - Cons: size limitations of free storage, risk of storage site closing, needs a reliable internet connection, risk of being remotely hacked

- External Hard Drive/ SSDs
  - SanDisk, Samsung, Western Digital, Seagate, Crucial
  - Pros: Easy to use – drag & drop files, easily accessible on-site
  - Cons: hardware failure possible, on-site prone to physical risks, user-managed

- CD/DVDs, USB Flash Drive, NAS (network-attached storage) Device

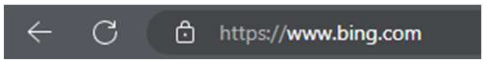
IT SECURITY

Basics of Data Encryption



Data Encryption on Website

- Ensure that the website runs on the HTTPS (hyper text transfer protocol secure)



- HTTPS websites have a Secure Socket Layer (SSL)
  - SSL certificates - encrypts the in-transit data and communications between website servers and website visitors
  - Are one of the most crucial encryption tools that will protect data from unauthorized access

- Purchase an SSL certificate a from trusted certificate provider: Symantec, GeoTrust, Sectigo, GoDaddy etc.

Data Encryption on Email

- Secure/Multipurpose Internet Mail Extensions (S/MIME) – a security protocol that digitally signs and encrypts emails
  - Industry standard for email encryption & signature by businesses

Steps to Encrypt an Email:

1. Get a Certificate
2. Install S/MIME control
3. Create a new message
4. Run or save the file
5. Encrypt and digitally sign outgoing messages
6. Verify the signature or a digitally signed message
7. Read a message

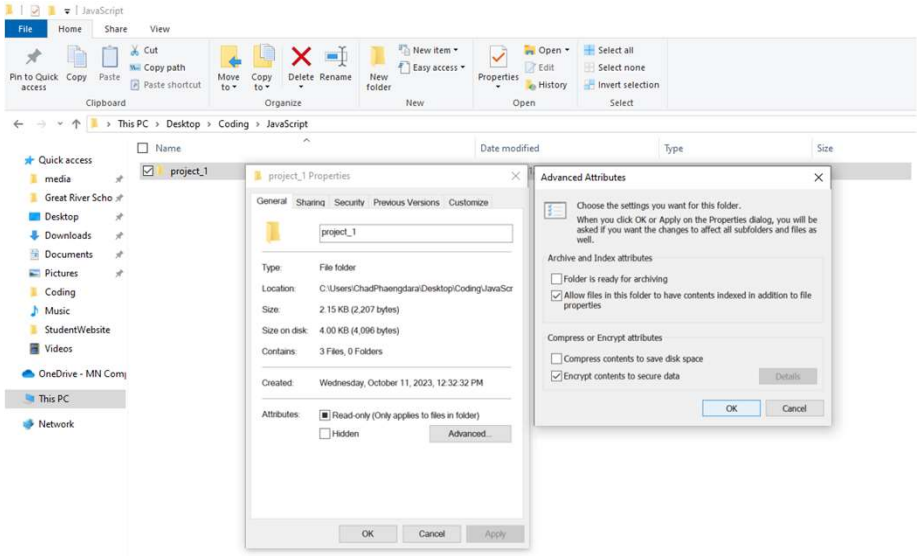
For an in-depth step-by-step guide:

- Encrypt messages by using S/MIME in Outlook Web App - Microsoft Support

Data Encryption on Computer

To encrypt a file on your computer:

1. Right-click: the file/folder you wish to encrypt
2. Select: Properties
3. Click: Advanced…
4. Check box: Encrypt contents to secure data
5. Click: OK
6. On Properties, Click: Apply
7. On Confirm Attribute Changes, select: “Apply changes to this folder, subfolders and files”
8. Click: OK
9. Encrypting File System Notification will appear
10. Select Back up now (recommended)
11. Run through the Certificate Export Wizard and select all defaults

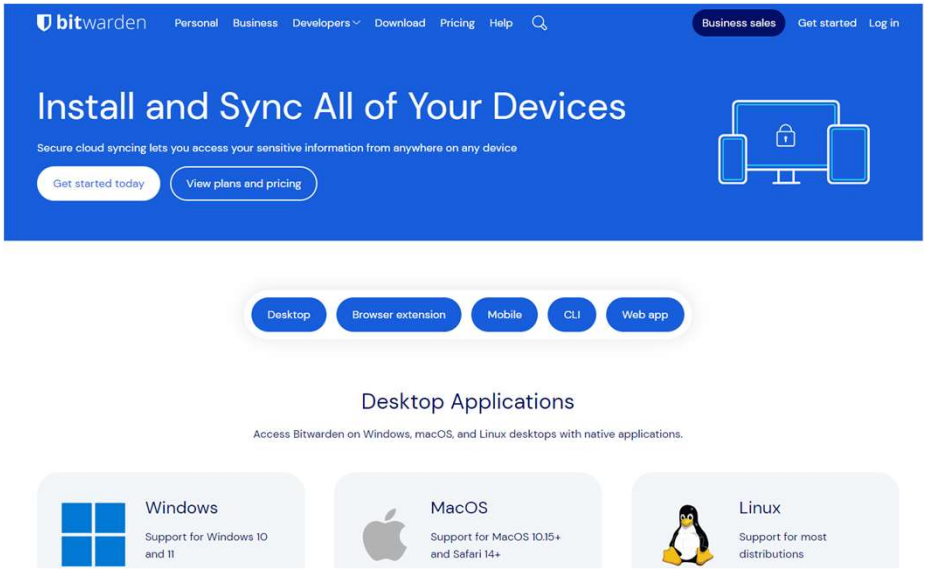


ACTIVITY

Password Manager

Activity 1: Download & Install Password Manager

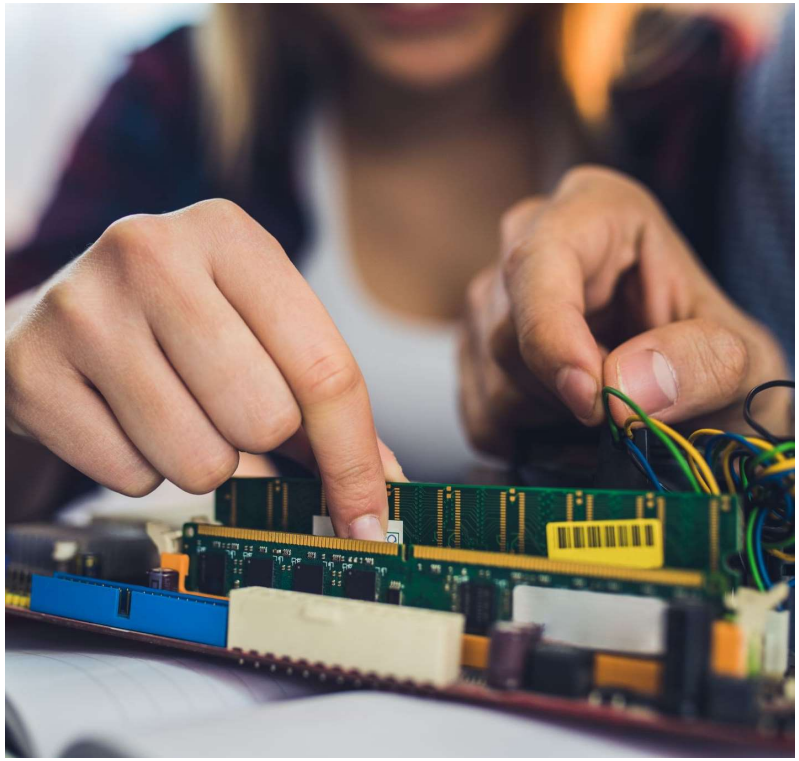
1. Navigate to: https://bitwarden.com/download/
2. Under Desktop Applications, Click: Windows
3. Run Installer
4. Setup your free account
5. Optional: Install bitwarden on your smartphone
    1. Accounts and passwords will sync in Realtime



WAREHOUSE

Warehouse Activity

- 1:30-3:00pm
- Parting/recycling
  - Review production numbers from 2/7
  - Assemble g-Force HPs
  - RAMs
  - HDDs & SSD



BREAK

5 minutes