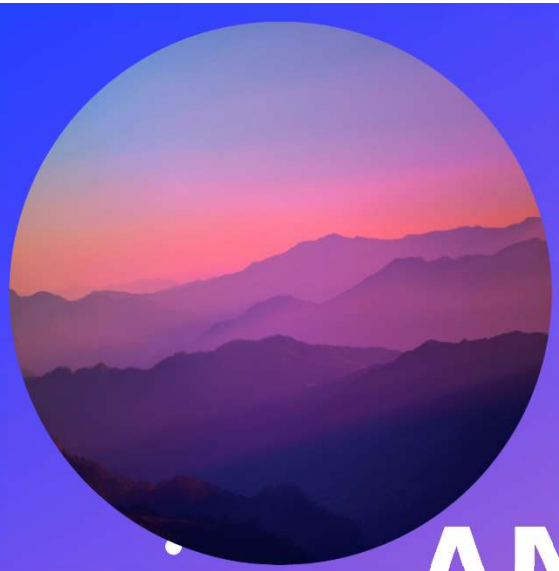
MINNESOTA TECH FOR SUCCESS

Week 11-12: IT Security

2/7/2024

Agenda

- **Announcements**
- **Classroom (25 min)**
  - Importance of IT Security
  - Everyday Security Threats
- **Break (5 min)**
- **Warehouse (1.5 hrs)**
  - Recycling



ANNOUNCEMENTS

Week 11

Announcements for 2/7

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

Values

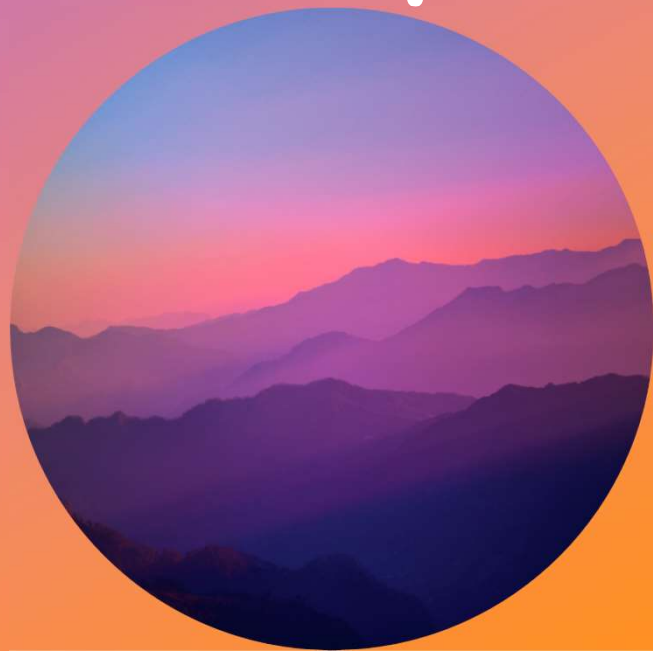
- **R**espect
- **A**ccountability
- **I**mprovement
- **S**teadfast
- **E**ncouragement

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

Why IT Security is Important



Importance of IT Security: Statistics

- There were an estimated 800,000 cyberattacks in 2023– with that number predicted to continue to rise annually
- Cybercrime was predicted to hit $8 Trillion in 2023 and grow to $10.5 Trillion by 2025
- FBI reported Phishing as the most reported type of cybercrime as of 2020
- Open-source code vulnerabilities have been found in 84% of code bases that can lead to exploits
- An estimated 300,000 new malware are created daily
- 92% of malware is being delivered via email
- Every 39 seconds, a threat actor targets a business's cybersecurity infrastructure

Importance of IT Security: Case Study – Insomniac Games

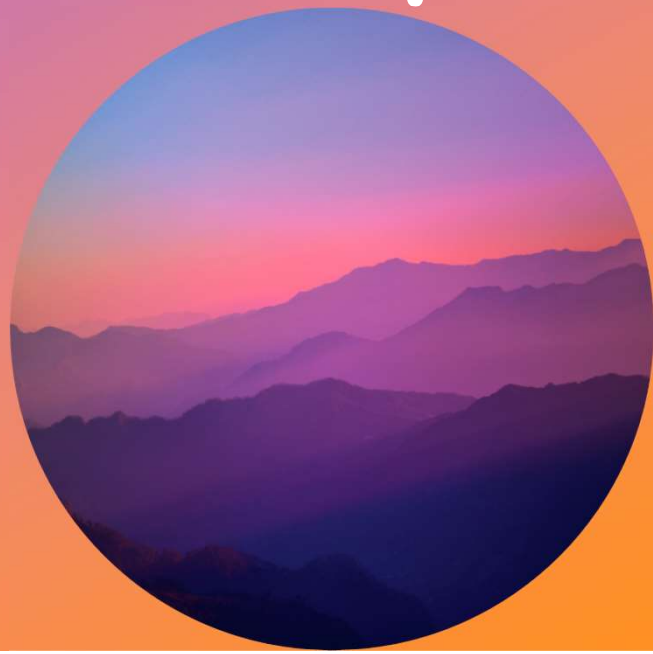
- December 12th 2023 – Announced that Insomniac Games data was held hostage by ransomware group Rhysida
- Wanted 50 bitcoin for the data ($2 million) – anyone could bid for it
- After 7-day deadline passed without a buyer, posted most of the hacked data online
- 1.67 TB of data (1.3 million files)
  - Marvel's Wolverine – design documents, casting information, level designs
- Affects non-disclosure agreements with major companies & studios
  - Slack communications, recorded videos of meetings
  - HR documents
  - Employee data & ID documents
- Over 400 employees impacted

Importance of IT Security: Why it matters to you and businesses

- Mitigate risk of data beaches & loss
- Protect customer, employee, and company data
- Adhere to compliance and standards
  - HIPAA (Health Insurance Portability and Accountability Act of 1996)
  - SOX (Sarbanes-Oxley Act of 2002)
- Maintain customer and public trust
- Avoid downtime
- Avoid financial losses
- Avoid reputational damage

IT SECURITY

Everyday Security Threats



Malware Definitions

- Malware – software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy
- Virus – malicious software or malware that replicates itself by modifying other computer programs or inserting its own code into them
  - Spreads from one computer to another and may damage data and software
- Trojan – malicious code or software that feigns legitimacy to take control, damage, disrupt, steal, or inflict harmful action on the data and network
- Ransomware – cyrptovirological malware that permanently block access to a victim's personal data until a ransom is paid
- Adware – malicious software that secretly installs itself on a device and displays unwanted advertisements and pop-ups
- Spyware – malware that collects user activity data without their knowledge
- Keylogger Monitors users' keystrokes

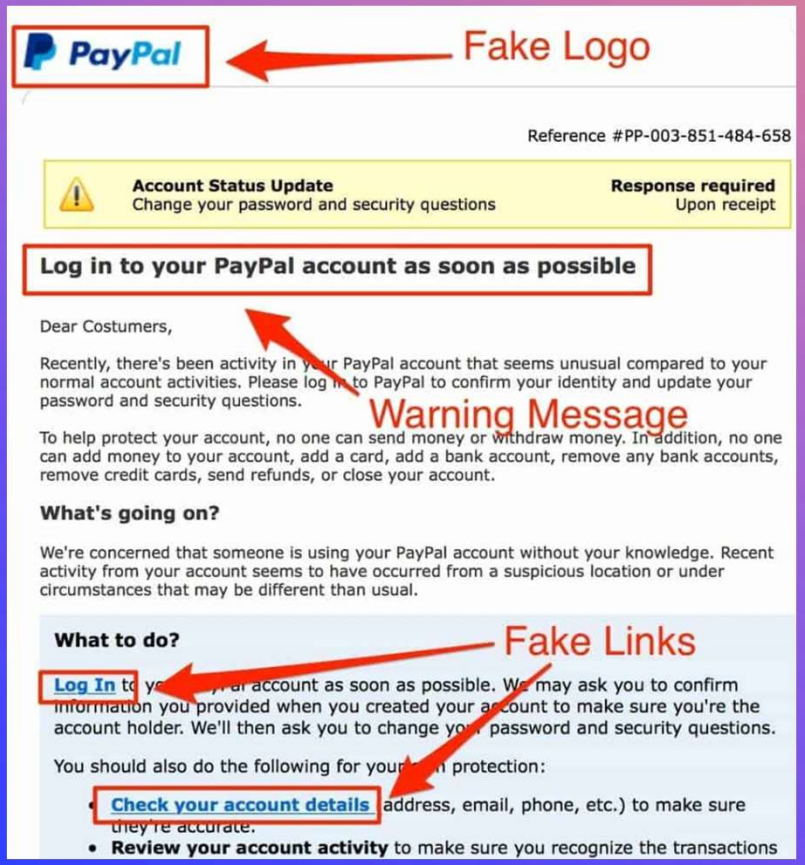
Cybersecurity Attack Definitions

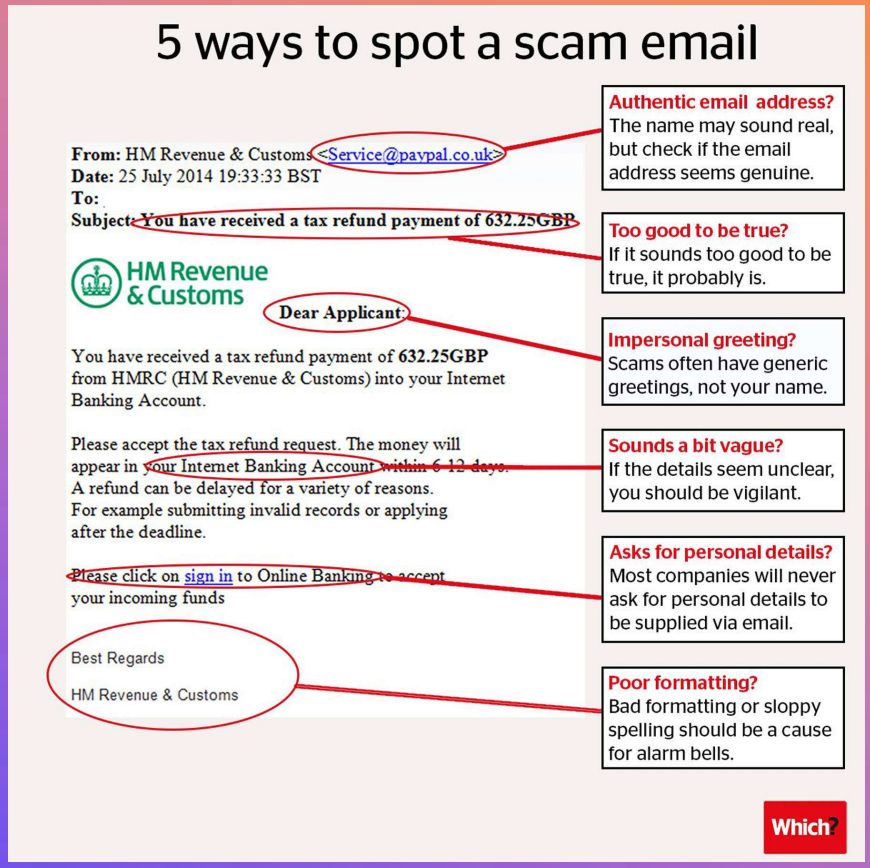
- DoS/DDoS – attack designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests
  - A distributed denial-of-service (DDoS) attack also seeks to drain the resources of a system. It is initiated by a vast array of malware-infected host machines controlled by the attacker
- Man-in-the-middle (MITM) - an attacker eavesdrops in on the middle of the data sent back and forth between two people, networks, or computers
- DNS Spoofing- hacker alters DNS (domain name system) records to send traffic to a fake or spoofed website where the victim may enter sensitive information that can be used or sold by the hacker
- Social Engineering – manipulation technique that exploits humans to erroneously provide access or valuables
- Phishing – social engineering or scam where attacker deceives victims into revealing sensitive information or installing malware

Types of Phishing Definitions

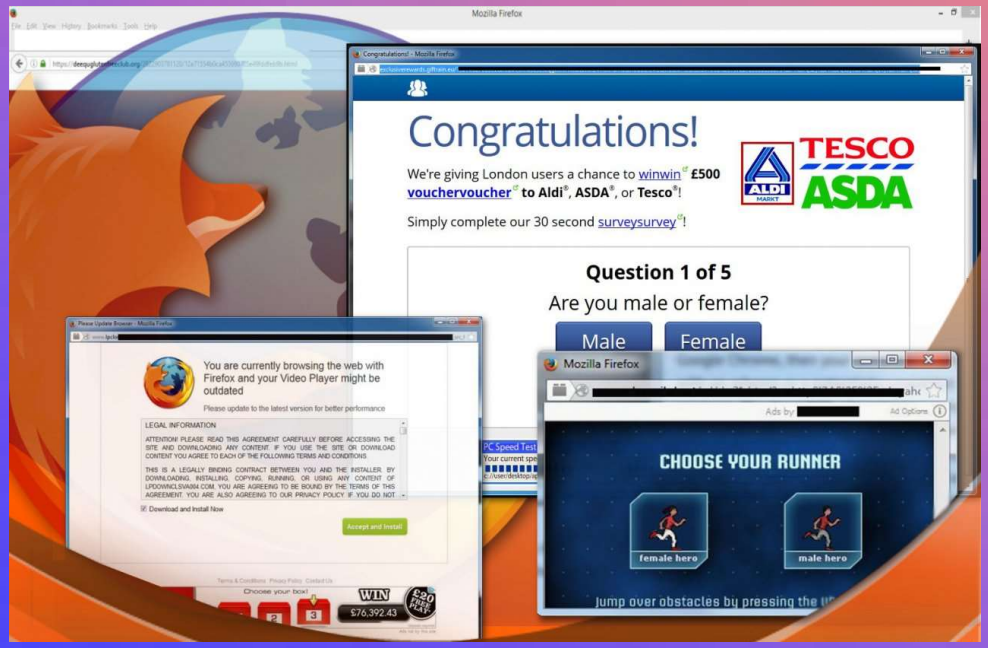
- Email Phishing – fraudulent email messages from imitators that seem to look like legitimate sources that are made to trick recipients into revealing sensitive information
- Spear Phishing – social engineering or scam where attacker deceives victims into revealing sensitive information or installing malware
- Whaling & CEO Fraud – attacks that target those in the C-suite or others in charge of the organization who are likely to possess valuable information, such as proprietary information about the business or its operations
- Clone Phishing – a real email message is cloned with attachments and resent, pretending to be the original sender
  - Attachments are replaced with malware that look like the original documents
- SMS Phishing (smishing) – social engineering attack that uses text messages to trick users into downloading malware, sharing sensitive information or sending money
- Page Hijacking- redirecting Web traffic that exploits engines where it creates a website that redirects site visitors or where an owner/creator loses control of their page

EXAMPLE


PayPal
Fake Logo
Reference #PP-003-851-484-658
Account Status Update
Change your password and security questions
Response required
Upon receipt
Log in to your PayPal account as soon as possible
Dear Costumers,
Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity and update your password and security questions.
Warning Message
To help protect your account, no one can send money or withdraw money. In addition, no one can add money to your account, add a card, add a bank account, remove any bank accounts, remove credit cards, send refunds, or close your account.
What's going on?
We're concerned that someone is using your PayPal account without your knowledge. Recent activity from your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.
What to do?
Fake Links
Log In to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to change your password and security questions.
You should also do the following for your protection:
Check your account details address, email, phone, etc.) to make sure they're accurate.
Review your account activity to make sure you recognize the transactions

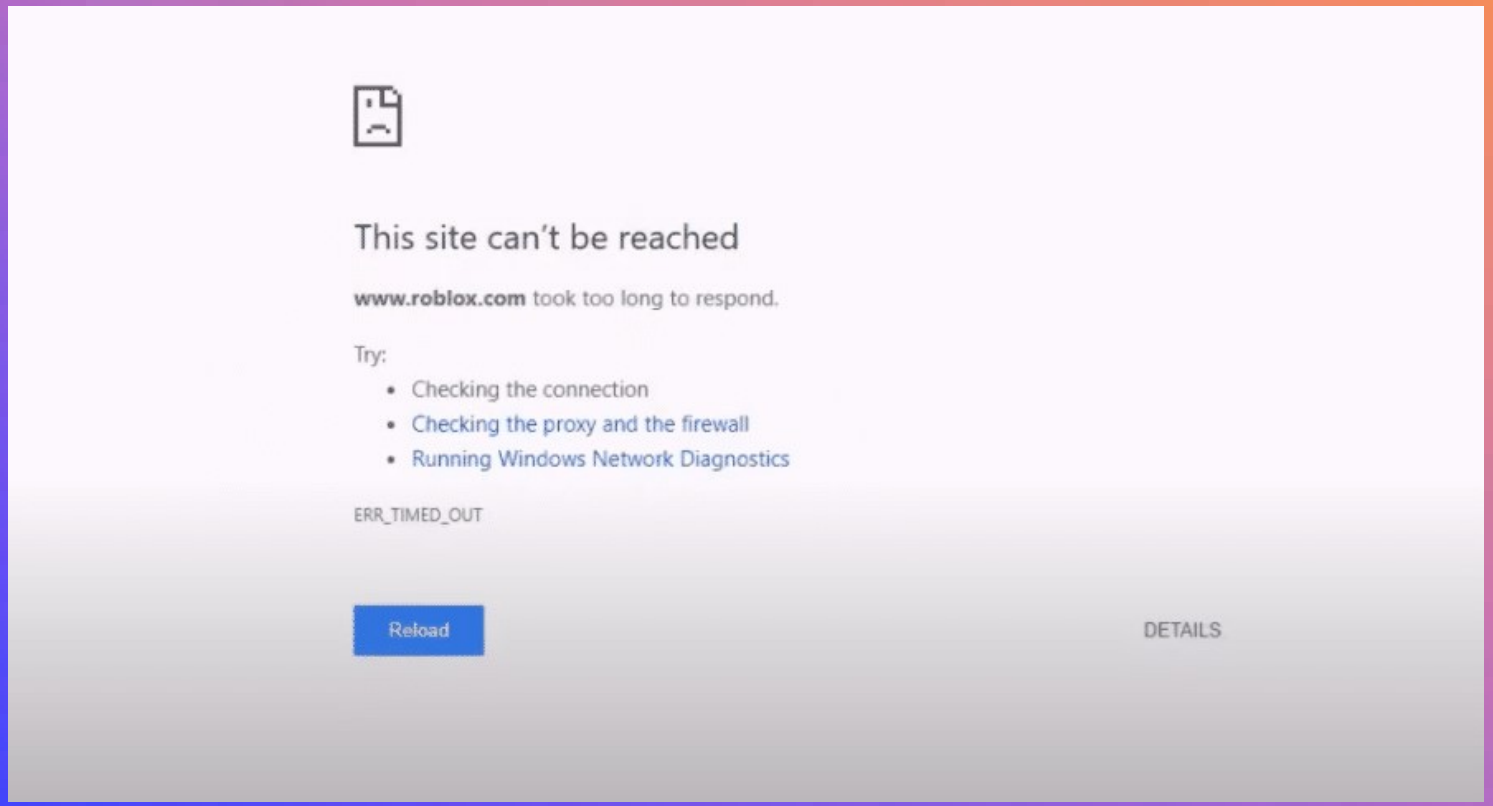

5 ways to spot a scam email
From: HM Revenue & Customs <Service@paypal.co.uk>
Date: 25 July 2014 19:33:33 BST
To:
Subject: You have received a tax refund payment of 632.25GBP
HM Revenue & Customs
Dear Applicant,
You have received a tax refund payment of 632.25GBP from HMRC (HM Revenue & Customs) into your Internet Banking Account.
Please accept the tax refund request. The money will appear in your Internet Banking Account within 6-12 days.
A refund can be delayed for a variety of reasons.
For example submitting invalid records or applying after the deadline.
Please click on sign in to Online Banking to accept your incoming funds
Best Regards
HM Revenue & Customs
Authentic email address?
The name may sound real, but check if the email address seems genuine.
Too good to be true?
If it sounds too good to be true, it probably is.
Impersonal greeting?
Scams often have generic greetings, not your name.
Sounds a bit vague?
If the details seem unclear, you should be vigilant.
Asks for personal details?
Most companies will never ask for personal details to be supplied via email.
Poor formatting?
Bad formatting or sloppy spelling should be a cause for alarm bells.
Which?

EXAMPLE


Mozilla Firefox
Congratulations!
We're giving London users a chance to winwin £500 vouchervoucher to Aldi, ASDA, or Tesco!
Simply complete our 30 second surveysurvey!
TESCO
ASDA
Question 1 of 5
Are you male or female?
Male
Female
You are currently browsing the web with Firefox and your Video Player might be outdated
Mozilla Firefox
CHOOSE YOUR RUNNER
female hero
male hero
Jump over obstacles by pressing the


http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer
CONGRATULATIONS!
You've been chosen to receive a FREE Gateway Desktop Computer!
Intel Pentium 4 Processor 2.66 GHz
256MB DDR-SDRAM, 80GB HD, 48x CD-RW
19-inch Color CRT Monitor (18-inch viewable)
Click Here to Claim Your FREE Desktop Computer!
FREE!
Microsoft Internet Explorer
Click OK to download our free software while browsing the site
OK
Cancel
POKER ON-NET
Download
Getting Started
Features
Contact Us
Help
> Current Events
Blackjack
Roulette
Slot Machine
Click Here!
Recycle Bin
start

EXAMPLE


This site can't be reached
www.roblox.com took too long to respond.
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_TIMED_OUT
Reload
DETAILS

Sources

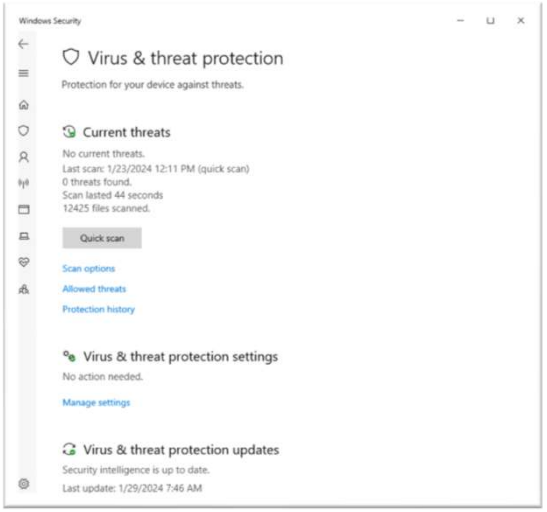
1. eSentire
2. OSSRA
3. packetlabs

ACTIVITY

Computer Scan

Activity 1: Scan your computer for Threats

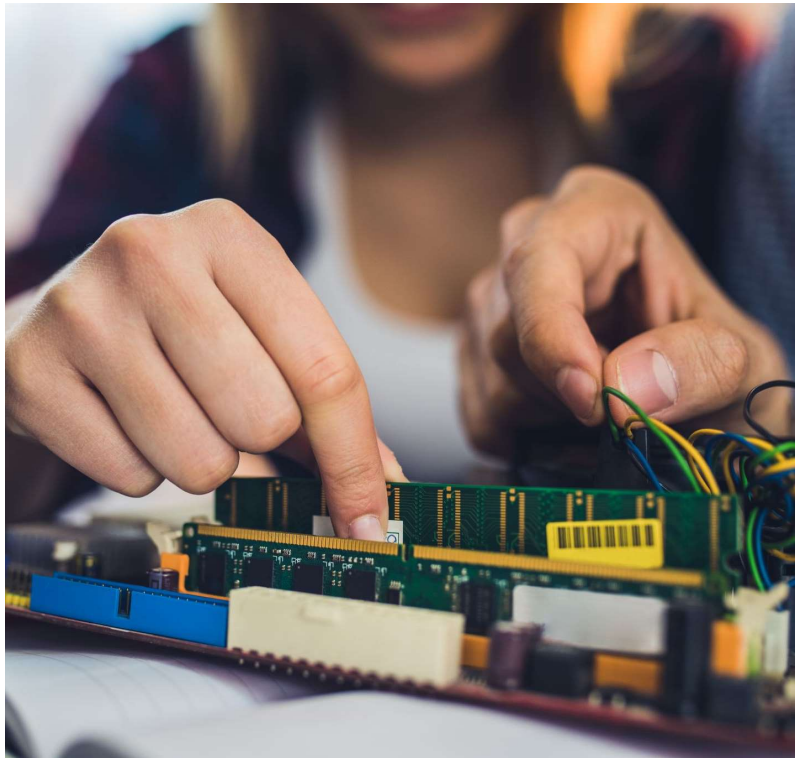
1. Windows search bar, Type: Windows Security
2. Open/Run: Windows Security
3. Click: Virus & threat protection
4. Click: Quick scan



WAREHOUSE

Warehouse Activity

- 1:30-3:00pm
- Parting/recycling



BREAK

5 minutes