JOSÉ RIZAL UNIVERSITY
Find your Inner Hero

husay rizal

Module 5 / Unit 2 / Using Best Practices

CHED AUTONOMOUS STATUS

Great Place To Work. Certified

ISO 21001:2018 TÜVNORD

Objectives

- Describe basic principles for hardening computer systems against attack.
- Distinguish between different types of malware and use anti-malware software effectively.
- Identify and mitigate spam and phishing threats.
- Install software patches and updates from secure sources.

Securing Devices

- **Device "hardening"** is the process of applying policies and configurations to make mobile devices, workstations, and network appliances more secure against attack.
- **Anti-Malware:** Essential software that protects against malware (malicious software) designed to damage a computer, steal data, or gain unauthorized access.
- **Patching/Updates:** The regular application of software patches is critical. Updates fix existing OS files, application software, driver software, and firmware, preventing them from being exploited by attackers.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

Security Software

- **Anti-Malware Suites:** Software designed to prevent, detect, and mitigate the effects of malware. In Windows 11, the built-in **Windows Security (Defender)** offers this comprehensive protection.
- **Signature-Based Detection:** Anti-malware programs use *virus definitions (patterns/signatures)* to recognize known malicious code.
- **Real-Time Protection:** This is the default and most critical setting, scanning files as they are opened, saved, or downloaded to provide immediate defense against threats.
- **Behavioral/Heuristic Protection:** Modern suites also analyze file behavior (heuristics) to detect new, unknown (zero-day) malware.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

Types of Malware

- **Virus:** Malicious code that replicates by attaching itself to a host file (programs, documents). The virus's harmful actions *(payload)* are only executed when the host program is run.
- **Worm:** Similar to a virus, but is *self-propagating* and does not require a host file. A worm typically spreads rapidly across a network by exploiting security vulnerabilities.
- **Trojan Horse (Trojan):** A malicious program that is deceptively disguised as, or hidden within, legitimate or desirable software to trick a user into executing it.

Types of Malware (cont.)

- **Ransomware:** A major modern threat where malware encrypts the victim's files, demanding a ransom payment (typically in cryptocurrency) to restore access. The best defense is a reliable, offsite backup.
- **Spyware:** Software installed covertly (without the user's knowledge) to monitor computer activity, capture keystrokes (keyloggers), and gather sensitive personal or financial information.
- **Rootkit:** A sophisticated type of malware designed to modify or replace core Operating System (OS) files at a low level. This allows the malware to mask its presence, making it extremely difficult for traditional anti-malware software to detect and remove.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

Types of Malware (cont.)

- **Adware:** Software that displays unsolicited pop-up advertisements or advertising banners to the user. It is often bundled with legitimate freeware during installation.
- **Botnet:** A network of computers (bots) that have been infected with malware and are remotely controlled by an attacker via a central command-and-control (C2) server. Botnets are often used to launch large-scale Distributed Denial of Service (DDoS) attacks.
- **Phishing:** A social engineering attack (not malware itself) where an attacker attempts to trick a user into revealing confidential information (passwords, PII, credit card details) by disguising themselves as a trustworthy entity via email, text, or phone call.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

JOSÉ RIZAL UNIVERSITY
Find your Inner Hero

husay rizal

Types of Malware (cont.)

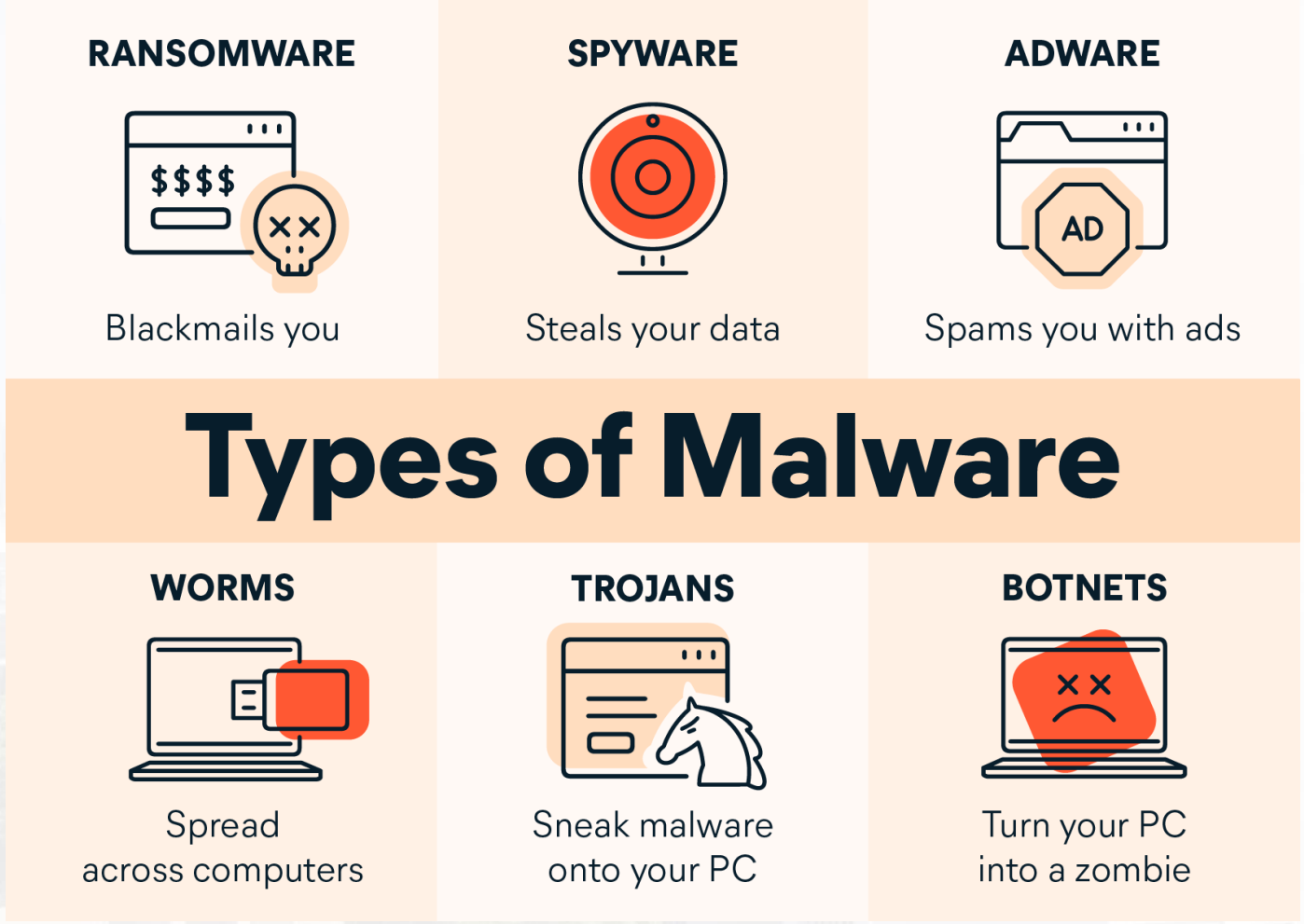


Image Source: https://www.avast.com/c-malware

Anti-Malware Software

- **Scans:** The process of inspecting files and memory for malicious code:
  - **Real-Time Protection:** The default mode, which continuously inspects files and memory as they are accessed or modified.
  - **On-Demand Scans:** Scans initiated manually by the user or scheduled to run at set times.
- **Malware Removal and Quarantine:** When malware is detected, the program attempts to clean (remove) the infection or place the file in quarantine (an isolated, inaccessible location) so it cannot harm the system.
- **Configure Exclusions:** System administrators can configure exclusions to prevent the scanner from checking specific files or directories, typically used for known safe application files to avoid performance impact.

Anti-Malware Software (Windows Security)

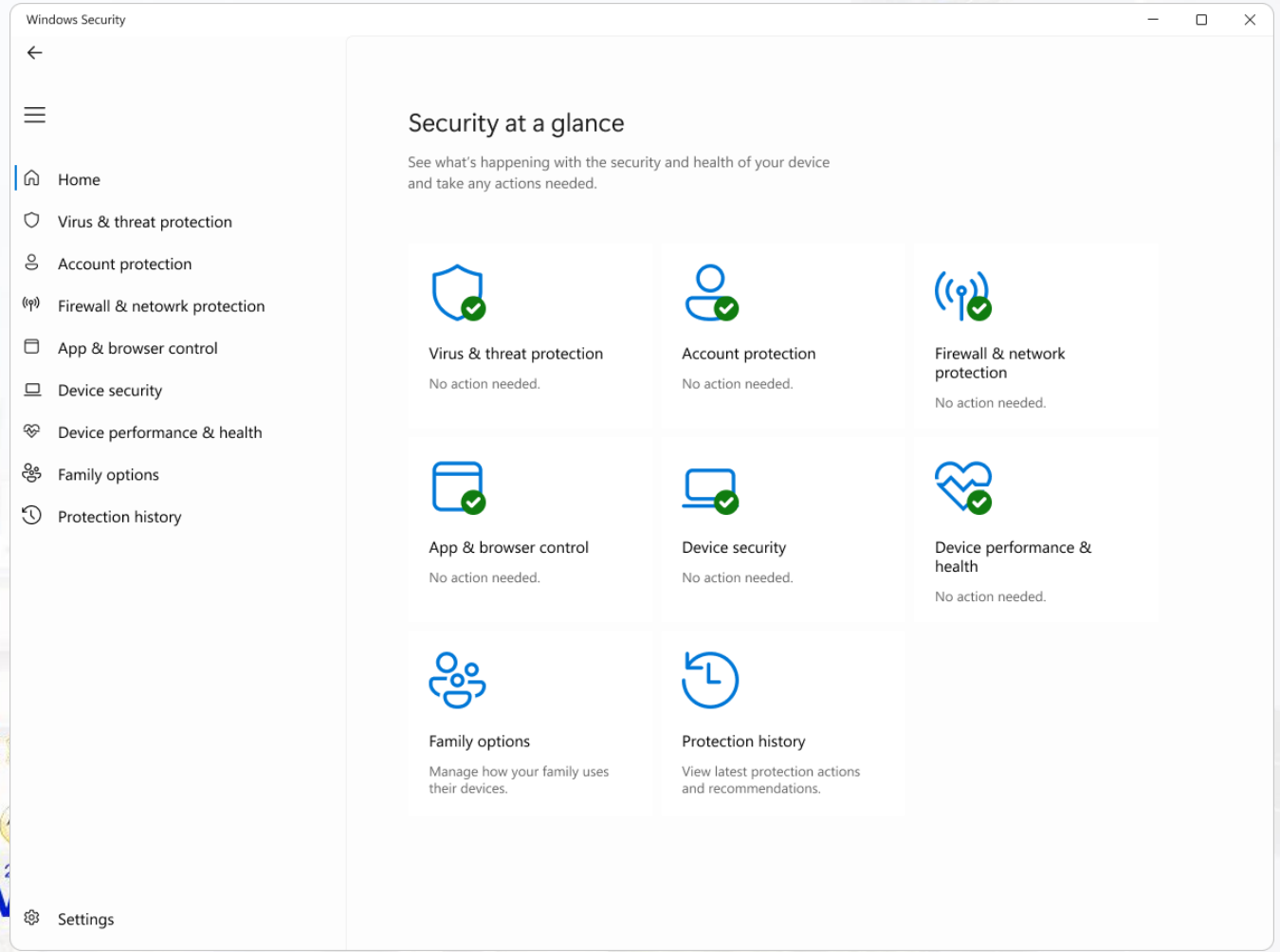


Image Source:
https://support.microsoft.com/en-us/windows/

Malware Removal

- **Run Anti-Malware Utility:** Initiate a full, up-to-date scan using a reliable anti-malware utility to identify and remove the threat.

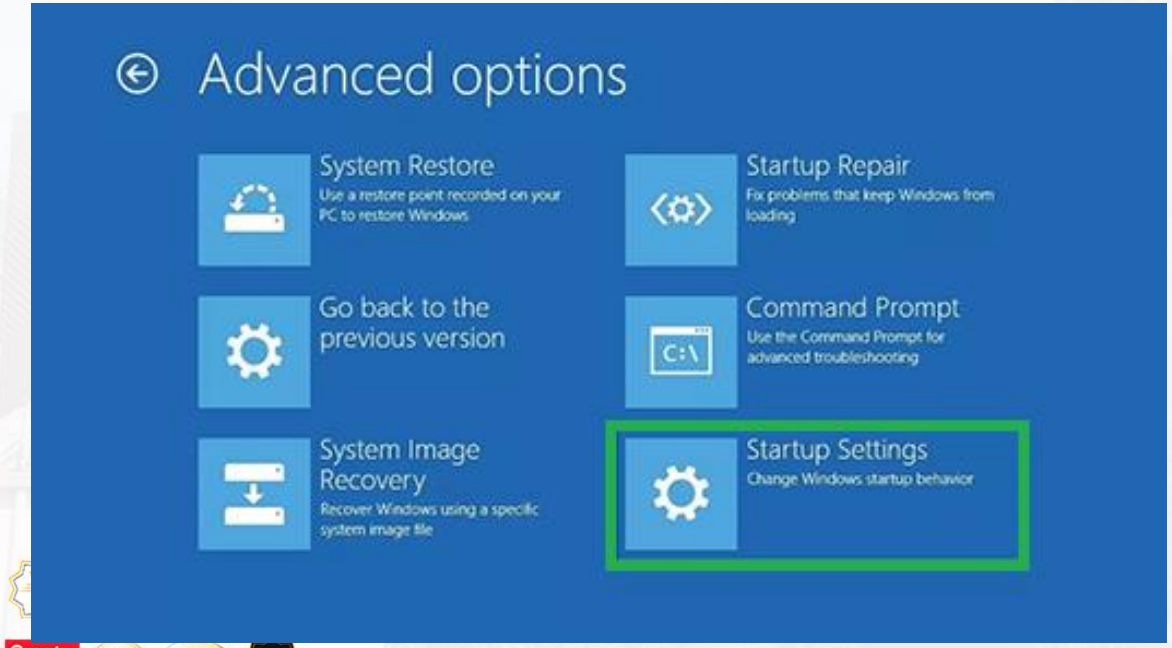


Image Source: https://www.tomsguide.com/

- **Use Safe Mode:** If malware prevents successful removal while the OS is running, the system should be booted into Safe Mode (which loads a minimal set of drivers and processes) to run the scan from a non-infected environment.
- **Bootable Scanner:** For severe infections that compromise the OS boot process, some vendors distribute bootable USB drives (replacing the older CDs) with an emergency scanner to clean the system before the OS loads.

Spam and Phishing

- **Spam:** Unwanted email (junk mail) that is often high-volume and unsolicited. While most is non-malicious advertising, spam poses a threat because it frequently contains malware attachments or phishing links.
- **Phishing:** A general term for social engineering attacks attempting to trick a user into revealing confidential information.
- **Modern Delivery Methods:** Phishing attacks are not limited to email:
  - **Smishing:** Phishing delivered via SMS (text message).
  - **Vishing:** Phishing conducted over voice call (Voice over IP or phone).

Phishing Types

- **Spear Phishing:** A highly targeted attack aimed at a particular individual or organization. It uses personalized, credible information (often gathered from social media) to make the attack more convincing.
- **Whaling:** A type of spear phishing attack specifically targeting senior executives or highly influential individuals within an organization (the "big fish").
- **Vishing (Voice Phishing):** A phishing attack conducted through a voice call (often using voice-over-IP or caller ID spoofing) to trick the victim into giving up sensitive information.
- **Smishing (SMS Phishing):** A phishing attack delivered via a text message (SMS), often containing a malicious link or a request for immediate action.

Windows Security (User Account Control - UAC)

- **User Account Control (UAC):** A core security feature in Windows 10 and **Windows 11** that prevents programs from obtaining full administrator privileges without explicit user approval.
  - When a legitimate application or a malicious process attempts to make changes requiring elevated access (e.g., installing software, modifying system settings), the **UAC dialog box** appears, prompting the user for authorization.
  - UAC helps prevent unauthorized changes to the operating system and limits the damage that can be done by malware.

Secure Logon and Authentication

- **Username/Password:**
  - **Passwords** must be strong (long, complex, unique) to prevent unauthorized access.
  - Users should never share passwords.
- **Multi-Factor Authentication (MFA):** Requires two or more different types of credentials to log in, significantly increasing security (e.g., a password (something you know) + a code from an authenticator app (something you have)).
- **Windows Hello:** In Windows 11, this feature provides modern biometric and PIN-based login, replacing traditional passwords with options like face recognition or fingerprint scanning.
- **Secure Screensaver Lock and Log Off:** Automatic screen locks prevent unauthorized users from accessing the system when the owner steps away ("lunchtime attacks").

Security Policy Examples

- **Password Policy:** Defines rules for creating secure passwords, including minimum *length and complexity* requirements. While older policies enforced *password aging* (frequent mandatory changes), modern best practice focuses on long, unique passwords protected by MFA.
- **Account Permissions:** Follow the principle of Least Privilege, ensuring that users and systems are not granted more access or permissions than are absolutely necessary to perform their required tasks.
- **Use of Multi-Factor Authentication (MFA):** Policy requiring the use of MFA for access to critical systems, user accounts, and remote access (VPN).

JOSÉ RIZAL UNIVERSITY
Find your Inner Hero

husay rizal

Safe Computing Practices

- **Web Filtering:** Utilize web filters or **Secure DNS** to block access to known malicious websites and phishing domains.
- **Email Safety:** Never open email attachments or click on links from unknown or suspicious senders. Always independently verify the sender's identity.
- **Secure Connections:** Always ensure the website uses **HTTPS** (Secure Sockets Layer/Transport Layer Security) when entering any sensitive information, such as passwords or financial data.
- **Password Management: Do not use the built-in "Remember Password" function** in web browsers; instead, use a dedicated, secure password manager application (e.g., LastPass, 1Password) or OS-level solution (like Windows/iCloud Keychain).
- **Personal Firewall:** Ensure the built-in **Windows Defender Firewall** (or a third-party equivalent) is active and configured to block unauthorized incoming connections, especially when on a public network.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

Patches, Updates, and Exploits

- Programming Errors: All complex software (applications and operating systems) contains programming errors (bugs).
- Patches: Small pieces of code designed to fix a specific bug or address a single problem.
- Updates: Generally refer to a larger bundle of patches released together, sometimes including new features (Feature Updates) or critical security fixes (Quality Updates).
- Security Vulnerability: A programming error or flaw that makes a system susceptible to attack.
- Exploit: The specific program, code, or method that takes advantage of a known security vulnerability to perform a malicious action.

Zero-Day Vulnerabilities and Service Packs

- **Zero-Day Vulnerability:** A serious security exploit that is actively being used by attackers before the software vendor knows about it or has released a patch to fix it. This is considered a critical threat.
- **Feature Updates:** A large, cumulative collection of patches, bug fixes, and sometimes minor feature updates, typically installed as a single package. The term *"Service Packs"* is used as a legacy term in Windows 10.

Patch Management

- **Patch Management:** The formal process of tracking, testing, and applying software updates and patches across all devices in an organization.
- **Automatic Distribution:** Modern OS and applications (including Windows 11) provide mechanisms (like Windows Update) to automatically distribute and install patches to protect the system.
- **Feature Updates / Quality Updates:** Microsoft uses these terms instead of Service Packs; Feature Updates (annually) introduce new functionality, while Quality Updates (monthly) provide security fixes.

JOSÉ RIZAL UNIVERSITY
Find your Inner Hero

husay rizal

Windows Update

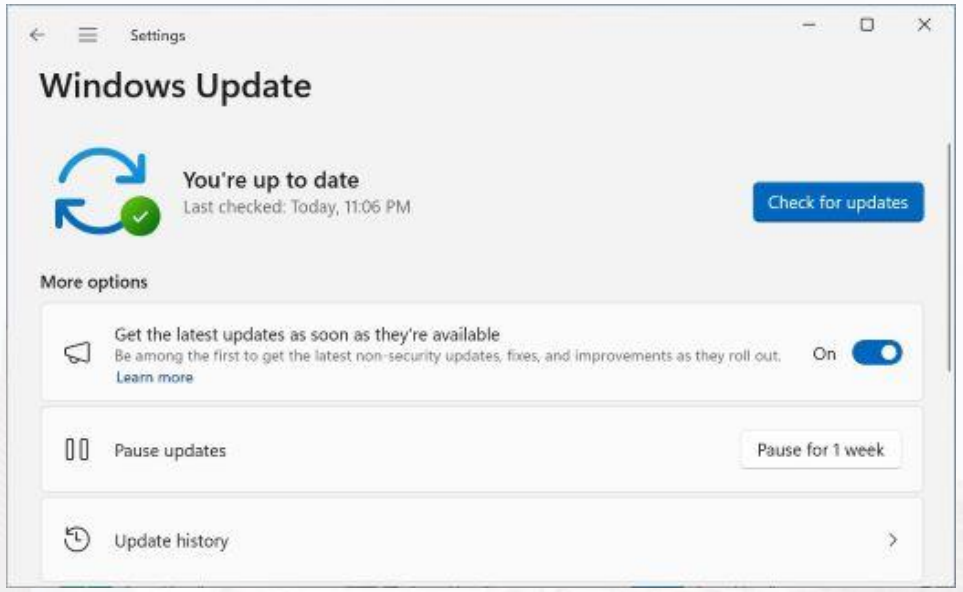


Image Source: https://support.microsoft.com/

- **Automatic Updates:** The Windows Update service automatically identifies, downloads, and installs system updates (Quality and Feature) directly over the Internet.
- **Active Hours:** Users can configure **Active Hours** in the **Windows 11 Settings** to specify when the device is typically in use, preventing automatic restarts for updates during those times.
- **Pause Updates:** Users have the option to temporarily *pause updates* for a short period, giving them control before critical updates are applied.

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD

Windows Update Scheduling and Frequency

- **Quality Updates:** Installed frequently (typically monthly) to provide security fixes and address small bugs.
- **Feature Updates:** Introduce new operating system functionality, typically released annually.
- **Servicing Channels** (Simplified in Windows 11): Microsoft has simplified its channels, primarily using:
  - **Windows Insider Program:** Allows users to opt-in for early access to pre-release Feature Updates (not recommended for production machines).
  - **General Availability Channel** (Formerly Semi-Annual): The standard channel for widespread deployment once updates are fully tested and ready for all devices.
  - **Long-Term Servicing Channel** (LTSC): Still available for specific Enterprise/IoT editions, offering highly stable builds with minimal feature changes over many years.

Other Essential Updates

- **Application Updates:** Software applications (e.g., web browsers, office suites, PDF readers) must be updated regularly, as they are a frequent vector for security exploits.
- **Anti-Malware Updates:** These are critical and typically occur multiple times a day:
- **Virus Definitions/Patterns/Signatures:** Updates the list of known malware for detection.
- **Scan Engine/Components:** Updates the core software that performs the scanning and analysis.
- **Driver Updates:** Updates for device drivers (e.g., for graphics cards, printers, Wi-Fi adapters) are often bundled with OS updates but may also need to be managed separately to address stability or security issues.

JOSÉ RIZAL UNIVERSITY
Find your Inner Hero

husay rizal

Review

- Describe basic principles for hardening computer systems against attack (e.g., using UAC, strong passwords, and Least Privilege).
- Distinguish between different types of malware (Virus, Worm, Trojan, Ransomware, Spyware) and use anti-malware software effectively.
- Identify and mitigate spam and phishing threats (including Spear Phishing, Vishing, and Smishing).
- Install software patches and updates from secure sources (e.g., using the Windows Update service in Windows 11).

Great Place To Work. Certified
ISO 21001:2018
TÜVNORD