A PRACTICAL GUIDE TO SOFTWARE SECURITY

BY NYAJHA OLIVE

WHAT IS SOFTWARE SECURITY?

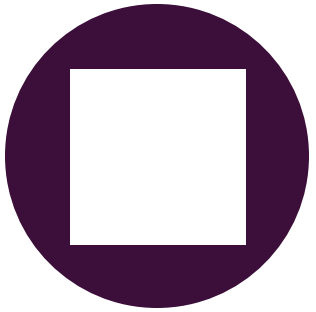
- Software security is a collection of methods used to protect computer programs and the sensitive information handled by them against malicious attacks.
- This protects company data, systems, and reputation
- Without it, vulnerabilities = open doors for attackers

IMPORTANCE FOR COMPANY

DATA BREACHES → LOSS OF SENSITIVE INFO

FINANCIAL LOSS → RECOVERY COSTS, LAWSUITS

REPUTATION DAMAGE → LOSS OF CUSTOMER TRUST



WORK DELAYS → SYSTEMS GO DOWN OR STOP WORKING

COMMON SOFTWARE VULNERABILITIES

Some of the biggest issues that lead to attacks are:

- Phishing emails - Fake emails tricking users into clicking links
- Malware - Malicious software that damages or locks systems
- SQL Injection - Attackers insert malicious code into databases
- Cross-Site Scripting (XSS) - Hackers inject scripts into websites
- Weak passwords - Easy-to-guess passwords

REAL-WORLD SECURITY BREACHES

1. Target (2013) – Malware Attack (Phishing + POS Malware)

- Attackers got in through a phishing email sent to a third-party HVAC vendor.
- Installed malware on Target's payment systems and stole 40 million card numbers.
- Showed how one weak partner can affect an entire company.

2. WannaCry (2017) – Ransomware Attack

- Spread globally through a Windows vulnerability called EternalBlue.
- Locked users out of their files and demanded Bitcoin payment to restore access.
- Affected 150+ countries, hitting hospitals, banks, and government systems.

3.Yahoo (2013–2014) – Data Breach / Credential Theft

- Hackers stole 3 billion user accounts by exploiting weak passwords and outdated security.
- Names, emails, and passwords were exposed.

4. Equifax (2017) – Software Vulnerability Exploit

- Hackers used an unpatched flaw in Apache Struts.
- Stole personal data from 147 million people.
- This shows that you should always keep systems updated.

WHY SOFTWARE SECURITY MATTERS TO THE COMPANY

A single breach can cost a company millions and destroy trust.

Example: The 2017 Equifax breach cost over $700 million.

Security issues can lead to:

- Legal penalties
- Lost customers
- Expensive recovery
- System downtime

BEST PRACTICES FOR NON-TECHNICAL STAFF

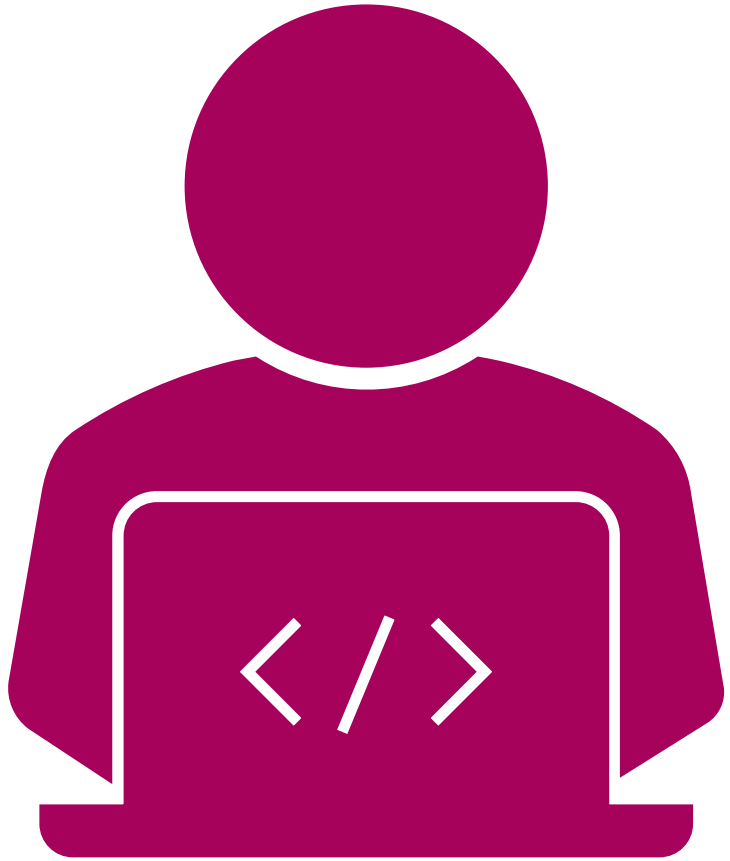
Even if you're not in IT, you can help protect the company by:

- Using strong passwords and MFA
- Watching out for phishing emails
- Avoiding unknown links or attachments
- Reporting anything suspicious to IT right away

BEST PRACTICES FOR TECHNICAL TEAMS

Tech teams should:

- Use secure coding (validate inputs, handle errors safely)
- Test software for weaknesses
- Keep systems and libraries up to date
- Encrypt sensitive data so it can’t be stolen



CONCLUSION

- Software security protects data, money, and reputation
- Common risks: phishing, malware, and weak passwords
- Staying safe means being aware and using smart habits
- A little caution goes a long way in keeping the company secure.

REFERENCES

- Bing. (n.d.). *Best practices for non-technical staff*. Microsoft Bing Search. https://www.bing.com/search?q=Best+Practices+for+Non-Technical+Staff&FORM=HDRSC1
- GeeksforGeeks. (2024, July 17). *What is software security? Definition and best practice*. https://www.geeksforgeeks.org/ethical-hacking/what-is-software-security-definition-and-best-practice/
- Microsoft. (2024). *Best practices for secure coding*. Microsoft Learn. https://learn.microsoft.com
- National Institute of Standards and Technology. (2023). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. https://www.nist.gov/cyberframework
- Symantec. (2024). *Cybersecurity threat report*. https://symantec.com