Cybersecurity Awareness “Best Practices”

> Today, we will introduce some Best Practices in Cybersecurity used to increase awareness about Cybersecurity to safe your organization and yourself from being compromised:
>
> 1- Password Management.
> 2- E-mail Security.
> 3- Social Engineering.
> 4- Data Privacy.
> 5- Software Updates.

▼ 1- Password Management.

> Creating and maintaining strong passwords is foundational to cybersecurity.

Best Practices To Create a password:

1. Hard to Guess & Easy to Remember.
2. Length Over Complexity.
3. Misspell Words on Purpose.
4. Avoid Common Words and Phrases.
5. Don’t Use Personal Information.
6. Avoiding Password Pitfalls.
7. Regularly Change Your Passwords.

Benefits of using a Password Manager:

1. Convenience.
2. Autofill.
3. Minimization of password reuse.
4. Stronger Passwords.
5. Increased Security.
6. Password Mobility.

▼ 2- E-mail Security.

> Phishing is the number one attack vector for compromising organizations, leading to data breaches. Even today it seems that email security is always afterthought when it really should be a top priority.

Best Practices to avoid Phishing Attacks:

1. Use Spam Filter.
2. Use Data Loss Prevention security control.
3. Use E-mail Scanning.
4. Train employees to spot and respond to malicious emails that bypass any technical defenses that are put in place.

▼ 3- Social Engineering.

> Social engineering attacks exploit human psychology to deceive individuals into divulging confidential information or performing harmful actions.

Some Techniques used in Social Engineering:

1. Pretexting.
2. Baiting.
3. Tailgating.

Best Practices Used to avoid Social Engineering Attacks:

1. Verify unexpected requests for information.
2. Always check unusual communications
3. Avoid sharing personal or organization information over phone or email or on social media platforms

▼ 4- Data Privacy.

> Protecting personal and organizational data is essential to maintaining trust and compliance with privacy regulations.

Best Practices:

1. Limit the amount of personal information shared online, and only provide necessary details to trusted sources.
2. Use ACLs.
3. Encrypt sensitive data both in rest or in transit.
4. Review third-party applications that access your data and revoke permissions that are not necessary.

▼ 5- Software Updates.

> Keeping software updated is critical in defending against vulnerabilities. Cybercriminals often exploit outdated software, as security patches frequently address known security flaws.

Best Practices:

1. Enable automatic updates wherever possible
2. Check for updates regularly for essential software, including operating systems, browsers, and antivirus programs.
3. Remove any app or software that you no longer use.
4. Set a patch management policy if in organization.