

Basic Digital Safety



Ensuring a security is crucial, in today's era, especially in the workplace where confidential data is frequently exchanged and stored. Here are some key recommendations to protect yourself and your workplace from threats:

1. Effective Password Management

It's important to use different passwords for each account. Opt for a mix of letters, numbers and special characters while avoiding information like birthdays or pet names. Consider utilizing a trusted password manager to handle and create passwords.

Source: National Institute of standards and technology

2. Implement Two Factor Authentication

Whenever possible, activate 2FA as a security measure. This feature requires a form of verification, such as a code sent to your phone, e-mail or app along with your password.

Source: Cybersecurity and infrastucture securityAgency

3. Stay Alert to Phishing Attempts

Phishing emails will look like messages in an attempt to deceive people into disclosing sensitive details or clicking on harmful links such as viruses or soft-wares that can steal all your personal information from a simple password up to even your own home address or bank details. Always check for grammatical mistakes and requests for data.

Source: Federal Trade Comission

4. Maintain Software Updates

Regularly updating software and operating systems is essential to address security vulnerabilities. Ensure you set up updates whenever you can to stay protected from threats, in a timely manner.

Source: United States Computer Emergency Readiness Team

5. Using Secure Wi-Fi networks

Avoid connecting to Wi-Fi networks for work-related tasks because they may not have security measures. When dealing with information on networks make sure to use a virtual private network (VPN).

Source: National Cyber Security Centre



6. Securing Data Storage

Encrypt our data to prevent access. Make use of cloud storage services that offer encryption and access controls to keep your important documents and files safe.

Source: International Organization for Standardization

7. Employee Training and Awareness

Conduct regular training sessions on safety practices for all employees. Foster a culture of vigilance. Empower employees to report any suspicious activities that they may notice.

Source: National Institute of standards and technology

8. Plan for Incident response

Create an incident response plan that details the steps to follow in case of a security breach. Ensure all employees are familiar with the protocol and regularly test its effectiveness through practices and tests.

Source: National Institute of standards and technology

9. Establish Access Restrictions

Restrict entry to individuals with the job-related needs only. Set up access controls based on roles to ensure that employees have access required for their duties.

Source: International Organization for Standardization.

10. Stay Updated

Keep yourself informed about cybersecurity risks and developments by following cybersecurity news outlets and engaging in industry discussions and events.

Source: Cybersecurity and Infratstucture security agency

By incorporating these measures for safety you can significantly decrease the chance of cyber threats and safeguarding both yourself and your workplace from potential dangers. Remember, Online security is a shared responsibility, stay alert and secure