For SMEs

Information Security 5 To-dos

"We don't have any confidential information"

Actually, it is very likely that you do.

- Employee "My Number", addresses, payroll, etc.
- Customer/business partner contact information
- Transaction amounts and records with business partners
- Information such as new product design plans
- Confidential information from business partners

CONFIDENTIAL

"Cyber-attacks aren't that serious, right?"

This is not true. Cyber-atttacks can cause significant damage.

- Compensation for damages to victims, etc.
- Suspension of transactions, loss of customers
- Decreased inefficiency due to network shutdowns
- Lower employee morale

For organizations that do not know what to do about information security, start with the "5 To-dos" on the back of this page today.

See the reverse side

Information Security 5 To-dos

1 Always keep your OS and software up to date

Leaving your OS and software outdated can leave security vulnerabilities unresolved, increasing the risk of viruses that exploit these weaknesses. Make sure to apply security updates or use the latest versions of your OS and software.

Examples

- ● Run vendor-provided services such as Windows Update (for Windows OS) or Software Update (for macOS).
- ● Update the software you are using, such as Adobe Reader and your web browser, to the latest versions.
- ● Ensure that the software on your computer and the firmware of your router are up to date for remote work.

2 Install anti-virus software

There has been an increase in viruses that steal IDs and passwords, perform remote operations, and encrypt files without permission. It is important to install antivirus software and ensure that virus definition files (pattern files) are always kept up to date.

Examples

- ● Set up automatic updates for virus definition files.
- ● Consider implementing integrated security software.
- ● Make effective use of the security features that are built-in within your OS.
- ● Install antivirus software on devices used for remote work and ensure that virus definition files are kept up to date.

3 Strengthen your passwords

There is an increasing number of cases from unauthorized logins due to passwords being guessed, cracked, or leaked from web services. Make your passwords strong, long and complex and do not reuse them.

Examples

- ● Use passwords that are at least 10 characters long, making them as long as possible, and ensure they are complex by including uppercase letters, lowercase letters, numbers, and symbols. Avoid using easily guessable information such as names, phone numbers, birthdays, or simple English words.
- ● Do not reuse the same ID and password across multiple services.
- ● When using VPNs or cloud services during remote work, set a strong password and use multi-step or multi-factor authentication where possible.

4 Review data/file sharing settings

Misconfigured web services for data storage or network-connected multifunction printers are leading to an increasing number of data exposure incidents. Ensure that servers and networked devices are shared only with people who are allowed to access them.

Examples

- ● Limit the sharing scope of web services, network-connected multifunction printers, cameras, and hard disks (NAS).
- ● Promptly change (or delete) settings when employees are transferred or terminated.
- ● Do not share computers used for remote work with others. If sharing is unavoidable, create a separate user account.
- ● When using public Wi-Fi outside the home or office, turn off file sharing on your computer.

5 Stay updated on possible threats and attacks

There has been an increase in sophisticated tactics where attackers send virus-laden emails pretending to be business partners or associates, or set up fake websites that resemble legitimate ones in order to steal IDs and passwords. It is important to be aware of the se threats and attack methods and to take appropriate countermeasures.

Examples

- ● Stay informed about the latest threats and attack methods by visiting the websites and checking newsletters of security organizations such as IPA (Information-technology Promotion Agency).
- ● Check the alerts provided by the internet banking and cloud services you are using.
- ● During remote work, administrators should provide timely warnings to employees, and employees should promptly report any security concerns.

IPA 独立行政法人情報処理推進機構
Information-technology
Promotion Agency, Japan（IPA）

E-mail isec-pr-nw@ipa.go.jp URL https://www.ipa.go.jp/en/

SECURITY ACTION

SECURITY ACTION ★

URL https://www.ipa.go.jp/en/about/activities/security-action.html

2025.5 Version