15 Ways to Protect Against Cybercrime

Security Assessment

Start with a security assessment to review any vulnerabilities, out-of-date systems, and other risks. Make note of your last security assessment.

Encryption

Use encryption wherever possible to keep data protected in transit and at rest - making it unreadable to unauthorized users.

Multi-Factor Authentication

Enable multi-factor authentication as an additional layer of security for any and all online accounts, including banks, cloud-services, and more.

Awareness Training

Keep your staff members trained on the latest threats, including how to spot them and mitigate risks, as well as constantly updating them on policies and procedures.

Security Policy

Create and enforce a security policy that outlines expectations in terms of password best practices, what cloud-based services are allowed, and how to operate on the network.

Workstation Updates

All workstations should be updated with the latest patches, updates, and bug fixes right away. This should be automated to protect against attacks.

Data Backups

Data should be backed up in two places: an onsite appliance and in the cloud to ensure recoverability in the event of a ransomware attack or other form of loss. Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit

Spam Protection

Use an anti-spam software that minimizes the risk of any potential phishing attacks coming through to your inboxes.

Access Control

Take measures to limit user access on an “as-needed basis” and set user screen time outs to prevent the risk of unauthorized access to sensitive data.

Endpoint Security

Implement an enterprise-grade endpoint security suite that protects against all sorts of threats, including malware, viruses, and ransomware attacks.

Dark Web Monitoring

Take advantage of dark web monitoring to scan the dark web for any potential login credentials or sensitive information that have been posted for sale.

Mobile Security

Be aware of the risk of mobile devices, especially employees using personal mobile devices for work purposes. Set up policies via mobile device management software to minimize the risks.

Web Security

A cloud-based web gateway security solution should be used to detect threats as they emerge from the internet - blocking them before they reach your end-users.

SIEM

Take advantage of a security information and event management (SIEM) solution that uses big data engines to review and analyze all security logs from devices.

Firewall

Implement a firewall with intrusion detection and intrusion prevention features enabled to secure traffic, then send all log files to the managed SIEM.

BONUS

Cyber Insurance

If you don’t already have cyber insurance that protects you against damages in the event of an attack, look for a policy that suits your needs.

Integrated365
7460 Warren Parkway Suite 100 Frisco, TX 75034
(469) 634-7653 | info@integrated365.com | www.integrated365.com