

Security Basics for Customers

SECURITY BASICS CHECKLIST

Threat actors love to find and exploit low-hanging fruit. Make their job harder by following these cybersecurity basics.

Draft an incident response plan.

- Print the plan as well, as your network may be down when you need it

Draft an information security policy.

Enable multi-factor authentication (MFA) on all critical systems.

- Email
- Remote access
- Third-party web applications

Adopt a password management solution.

- Use unique, complex passwords for all systems

Implement cybersecurity awareness training.

- Monthly training on cybersecurity topics
- Monthly phishing simulation

Accomplish defense-in-depth with the right security tools.

- Next-generation antivirus
- Managed endpoint detection and response
- DNS filtering
- Persistence detection
- Next-gen firewall with an intrusion detection system (IDS)

Implement a backup solution that is offsite and segregated from the environment.

- Scheduled disaster recovery (DR) testing

Update your line of business software.

- Under an active support agreement

Implement data integrity/access protection.

- Defined security groups for access
- Device encryption
- Encrypted data transmission outside the network
- Automatic locking of endpoints
- Least privilege access enforced