

SECURITY SOLUTION TIPS

INTERNET SECURITY

- Monitor traffic to your website and online presence
- Identify vulnerabilities hidden in your web applications
- Arrange for closing of vulnerabilities & issues identified



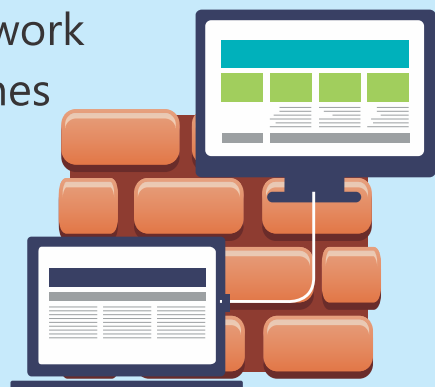
ONLINE EMPLOYEE

- Limit access to relevant websites and applications
- Restrict network access to personal devices
- Limit use of admin and privileged account(s)



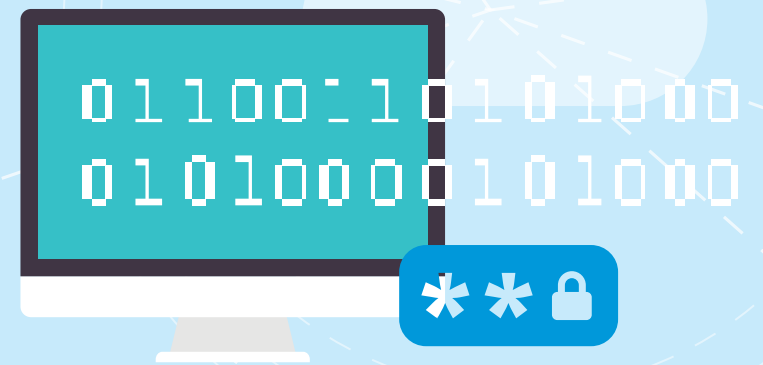
NETWORK SECURITY

- Use strong password policy on all devices – lengthy, complex, to be regularly changed
- Secure or block the open ports of network devices routers, switches, WiFi, etc.
- Use firewall, IDS/IPS or such solutions to protect your network
- Segregate zones for isolating internal system from internet (DMZ)
- Monitor and analyze network traffic for possible breaches



DEVICE/SYSTEM SECURITY

- Regular update antivirus, OS, patches, application software(s), etc.
- Regular monitor device and server logs to detect anomaly
- Configure devices & systems security
- Use encryption for data in rest and in motion
- Block use of malicious software and unsolicited programs/apps
- Control number of devices accessing network



PHYSICAL SECURITY

- Use strong identification and authentication techniques while providing physical access
- Control access to location where critical IT systems are located
- Monitor and review physical access to critical/sensitive areas

