Cybersecurity Cheat Sheet

1 Inventory Everything

- Track hardware, software, cloud services
- Prioritize assets by risk
- Use automated tools when possible

2 Patch Promptly

- Apply updates weekly or as soon as released
- Focus on high-severity vulnerabilities
- Don't forget firmware & third-party apps

3 Use Multi-Factor Authentication (MFA)

- Require MFA for email, cloud, VPN, remote access
- Use apps (e.g., Microsoft Authenticator, Duo) or hardware keys
- Avoid SMS if possible

4 Secure Your Endpoints

- Use advanced antivirus (MDR, EDR, or XDR)
- Keep definitions updated
- Cover laptops, mobile devices, and remote users

5 Train Your People

- Conduct regular phishing simulations
- Deliver bite-sized training modules
- Make security part of onboarding

6 Adopt Zero Trust

- Assume breach. Verify everything.
- Limit user access to what's needed
- Monitor network activity

7 Encrypt Your Data

- Use encryption at rest (file systems, drives)
- Encrypt in transit (TLS, VPNs, email tools)
- Apply policies organization-wide

8 Back Up and Test

- Follow the 3-2-1 rule (3 copies, 2 media, 1 offsite)
- Automate backups
- Test recovery quarterly

9 Plan for Incidents

- Document your incident response plan
- Define roles, RTO (Recovery Time Objective), and RPO (Recovery Point Objective)
- Run tabletop exercises

Cyber Hygiene Quick Wins

- ✅ Enable MFA everywhere
- ✅ Uninstall unused software
- ✅ Disable unnecessary user accounts
- ✅ Run a vulnerability scan
- ✅ Teach team w/ simulated phishing
- ✅ Use a password manager

If Something Feels Off...

Don't click. Report it.
Contact your IT or cybersecurity partner ASAP
Document what happened

Resources

Software Solutions

intrustIT

Resources

Intrust IT - https://www.intrust-it.com/
Employee-owned IT support, cybersecurity protection, and cloud computing services.
NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
A flexible, risk-based approach to help public and private organizations manage cybersecurity.
CISA Cyber Essentials – https://www.cisa.gov/resources-tools/resources/cyber-essentials
A starter guide for small and mid-sized governments on building a basic cybersecurity strategy.
CIS Controls – https://www.cisecurity.org/controls/cis-controls-list
A prioritized list of technical and procedural best practices to reduce cyber risk.
Microsoft Secure Score – https://security.microsoft.com/securescore
A scoring tool that measures your Microsoft 365 security posture and provides improvement suggestions.
SecurityScorecard – https://securityscorecard.com
A platform that evaluates your external cybersecurity risk and grades your digital footprint.
KnowBe4 – https://www.knowbe4.com
Phishing simulations and security awareness training for employees.
Phishing.org – https://www.phishing.org
Educational resources to help users recognize and avoid phishing attacks.
Have I Been Pwned? – https://www.haveibeenpwned.com
Check if your email or passwords have been exposed in known data breaches.
TwoFactorAuth.org – https://www.twofactorauth.org
A directory showing which websites support two-factor authentication (and how to enable it).
Bitwarden – https://bitwarden.com
A secure, open-source password manager with MFA support.
1Password – https://1password.com
Another top-rated password manager that makes securing credentials easy for teams.
YubiKey by Yubico – https://www.yubico.com/
A physical security key for strong two-factor and passwordless login.
Veeam – https://www.veeam.com
Backup, recovery, and replication software, widely used in public sector IT.
Backblaze – https://www.backblaze.com
Cloud backup service with easy setup for personal and business systems.
VeraCrypt – https://www.veracrypt.fr
A free, open-source tool for encrypting files, folders, or entire drives.
FBI IC3 – https://www.ic3.gov
The FBI's official channel to report cybercrimes and online fraud.
CISA Alerts (US-CERT) – https://www.cisa.gov/news-events/cybersecurity-advisories
Up-to-date security alerts and vulnerability reports for the U.S. public sector.
OpenDNS (Cisco Umbrella) – https://www.opendns.com
Cloud-delivered DNS security that blocks malicious domains before connections are made.