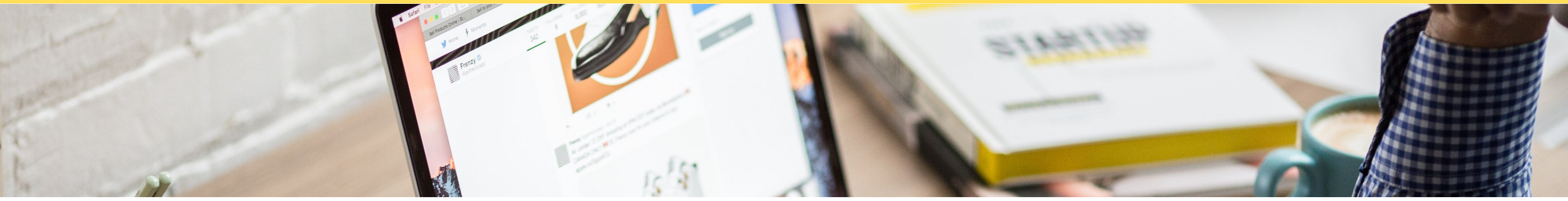
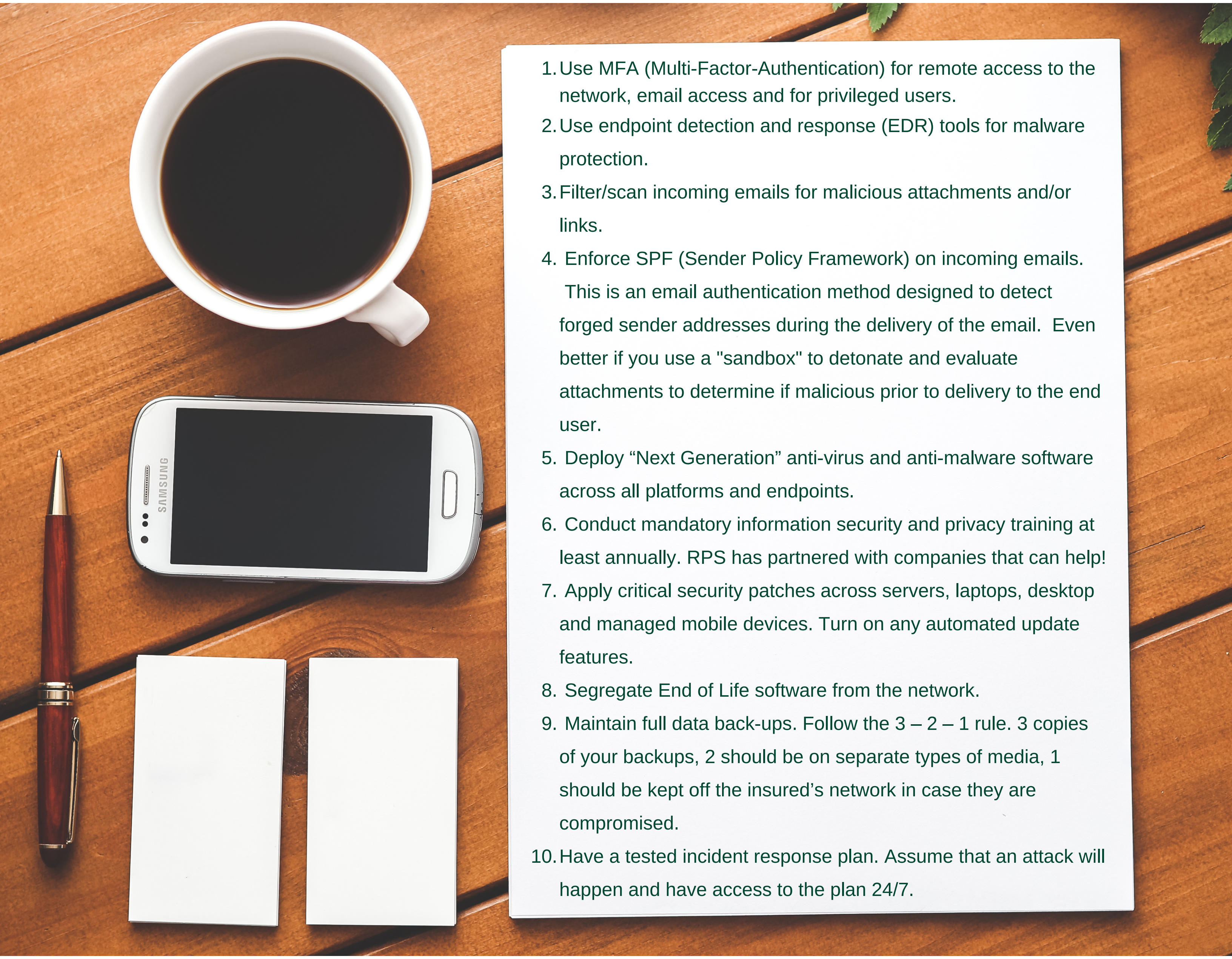


PREVENTING RANSOMWARE - BEST PRACTICES



1. Use MFA (Multi-Factor-Authentication) for remote access to the network, email access and for privileged users.
2. Use endpoint detection and response (EDR) tools for malware protection.
3. Filter/scan incoming emails for malicious attachments and/or links.
4. Enforce SPF (Sender Policy Framework) on incoming emails. This is an email authentication method designed to detect forged sender addresses during the delivery of the email. Even better if you use a "sandbox" to detonate and evaluate attachments to determine if malicious prior to delivery to the end user.
5. Deploy “Next Generation” anti-virus and anti-malware software across all platforms and endpoints.
6. Conduct mandatory information security and privacy training at least annually. RPS has partnered with companies that can help!
7. Apply critical security patches across servers, laptops, desktop and managed mobile devices. Turn on any automated update features.
8. Segregate End of Life software from the network.
9. Maintain full data back-ups. Follow the 3 – 2 – 1 rule. 3 copies of your backups, 2 should be on separate types of media, 1 should be kept off the insured’s network in case they are compromised.
10. Have a tested incident response plan. Assume that an attack will happen and have access to the plan 24/7.

"These best practices are not ensuring that any insured is guaranteed coverage nor listed in any order of importance. They have been gathered via various market feedback and provided to you as a resource for discussing your client's vulnerable areas"