PSA

IT SECURITY WHILE REMOTE

The unprecedented COVID-19 pandemic represents a golden opportunity for malicious actors. The FBI, Electronic Frontier Foundation, and Krebs on Security all caution that attacks are on the rise. We've assembled some resources below to help protect your remote workforce and your organization's bottom line.

Like you, Atomic Data has gone through a rapid change in how we conduct business. With change comes risk, especially when it comes to IT security. We're here to help you manage this risk and hope that you'll find value in the resources provided here.

- Jim Wolford, CEO

Best Practices

COVID-19 has forced many of us into a new way of life, both at home and at work. As the lines blur it's more important than ever to maintain certain best practices when it comes to your IT security.

- **Virtual Private Networks.** Beyond ensuring capacity for everyone, also be sure to monitor your network closely and keep VPN clients and firewalls up to date.
- **Home WiFi.** Password protect your WiFi, hide the SSID from public view, and split the guest network off to a different SSID. Deploying firmware updates promptly is also essential.
- **Antivirus.** Ensure any workstation that has access to your corporate network has an antivirus tool installed and running.
- **Patching.** New vulnerabilities, often leveraged to infiltrate networks, are found daily. Staying on top of security updates is a critical baseline for securing your network.
- **Multi-factor Authentication.** Turn on multi-factor for every possible service and use it always. The added layer of access control is quickly becoming the norm across many SaaS offerings.
- **DNS-based Protection.** Safeguard your users when they're not on VPN by deploying a DNS-based tool like Cisco Umbrella.

Quick Guide: IT Security for the C-Suite
Info Sheet: Patch Management
Info Sheet: Cisco Umbrella

Policies & Procedures

Though most policy manuals couldn't have accounted for COVID, certain policies and procedures have quickly become critical to ensuring business continuity. Providing written guidance on how to access cloud hosted resources from home, BYOD policies, VPN configuration, & backup best-practice enables your staff to rapidly transition and cuts your IT risk.

- **Prioritize.** Acceptable Use, Asset Management, Backup, Password Policy, Telecommuting, Security Incident Response, Disaster Recovery, and BYOD/Mobile Device policies should be developed and rolled out as soon as possible.
- **Distribute and train.** A policy binder printed years ago and stashed in a cubicle won't help you now. Consider GRC software to digitally distribute policies and ensure continual awareness and training.
- **Review and audit.** It's not enough to write these policies. Take the next step by reviewing them annually, auditing compliance, and remediating issues found during audits.

Info Sheet: Policy Advisory & Development

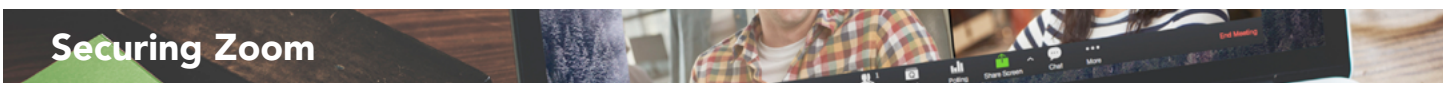
Social Engineering

Reports show a 600% increase in phishing attacks since February. This form of social engineering is designed to trick you and your already harried staff into a momentary lapse of judgement. Whether that means opening a malicious attachment or entering credentials on a convincingly fake Microsoft Office 365 login page, the intent is to infiltrate your network, deploy ransomware, or steal information/money. The best defense to social engineering is education and awareness.

- **Be suspicious.** Hover over links to determine the destination, review URLs carefully, and never open unexpected attachments.
- **Trust your gut.** If an email looks 'off' it probably is.
- **Keep it confidential.** Credit card numbers, passwords, & usernames should never be sent through email.
- **Test, educate, & repeat.** Employ phishing simulation to raise awareness, educate on incident handling, and hold users accountable.

Quick Guide: Phishing Awareness
Info Sheet: Security Awareness Consulting

Securing Zoom



Recent disclosures have brought certain Zoom Meetings vulnerabilities to light. Zoombombing, not so end-to-end encryption, and unwanted data sharing just to name a few. Some steps to take to secure your Zoom Meetings include:

- Ensure meeting passwords are required, including dial-ins.
- Enable the Waiting Room feature and disable Join Before Host.
- Implement Single Sign-On (SSO) and password complexity requirements

Blog: Zoom Security Advisory

Questions? We're available 24x7 to guide you with any of the above topics. Contact us at 612.466.2000 or info@atomicdata.com.