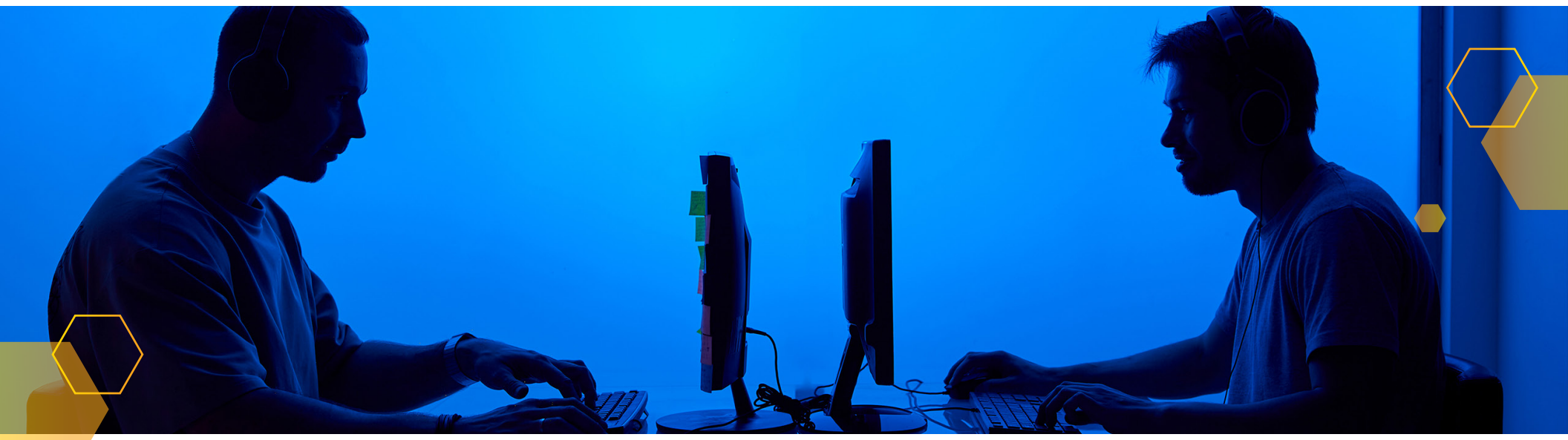
ATOMICdata

CYBERSECURITY BEST PRACTICES

# PUBLIC SERVICE ANNOUNCEMENT



## TECH GUIDANCE TO KEEP YOUR BUSINESS SAFE

Following the invasion of Ukraine, many businesses are concerned about the specter of increased Russian cyberattacks. Though to date the attacks have been 'more muted than expected', the threat of Russia lashing out at the U.S. remains. Plus, past incidents like NotPetya have shown that these attacks can have significant impact on unintended targets. Businesses of all sizes and industries should act now to ensure they are protected. Follow these fundamental best practices to step up your security posture.

### 1. Remain suspicious of email

Phishing remains the preferred method for hackers to breach company networks. 90 percent of successful cyberattacks start with phishing or spear phishing. Be suspicious of 'help Ukraine' scams requesting donations, including those with QR codes. Always verify the sender and hover over links before clicking. Bad actors will use slight variations of real web addresses to fool the user.

### 2. Patch Religiously

New vulnerabilities are constantly being located and patched. Fail to patch immediately and you increase your odds of infection from malware designed to exploit these vulnerabilities. Patch status should be reviewed regularly and updates automatically installed on all technology, including operating systems, applications, web browsers, mobile devices, network device firmware, industrial control systems, websites, etc. Automate patch management to drastically reduce time to patch and demands on your IT staff.

### 3. Step up your authentication

Complex passwords unique to each system and user, mandatory multi-factor authentication (MFA), sin sign-on (SSO), VPN, and zero-trust architecture are all essential components of a modern, secure network. Ensure you're consistently auditing critical systems like Active Directory/Azure AD and properly offboarding your employee and vendor accounts. Use tools like haveibeenpwned.com or password monitors to see if your info has been in a data breach.

### 4. Enable rapid detection

Malicious activity is rarely a singular event. There are multiple steps, early signs of which often go undetected for months or even years. Traditional, signature-based antivirus can no longer keep up with modern threats. Start with comprehensive asset discovery so you know what you have and where. Improve detection and response times with tools like Endpoint Detection and Response (EDR), Security Information & Event Management (SIEM), and Intrusion Detection.

### 5. Get redundant

Assess what systems are critical, then determine your recovery point (RPO) and recovery time objectives (RTO). For less critical systems, deploy and test backup solutions for both on-premises and cloud environments. For essential systems, implement redundant disaster recovery solutions that enable a rapid return to normal operations in the event of a security incident or outage.