MULTI-FACTOR AUTHENTICATION

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is an electronic authentication method requiring two or more security factors to be successfully verified prior to granting access to a system or network. The best practice is to implement MFA for remote network and email access, as well as local administrative and privileged access.

Things You Know

Including passwords, PINs, passphrases, and answers to security questions.

Things You Have

Including a security token or badge, a verified smartphone with an authentication app (like Google Authenticator or Duo), text confirmations, physical security objects like a USB key.

Things You Are

Including fingerprints, voiceprints, and biometric measurements like hand or face geometry.

Did You Know?

MFA can block as much as 99.9% of cyber attacks.

Cyber attacks against businesses continue to surge. In 2020, the FBI reported cyber crime incidents are up 70% and the costs organizations may face are crippling. The average ransom payment alone is $155,000 which does not include the additional expenses associated with business downtime, systems restoration, and reputational harm. While there is no silver bullet to protect yourself against these evolving threats, MFA has become a fundamental control every business should have in place.

Continued on next page...

Why Does This Matter?

The sophistication of hackers and cybercriminals makes it relatively easy to steal a valid user's login credentials. However, if you require more security access factors, the attackers need to steal more credentials.

For example, a user falls victim to a phishing scheme and gives up their username and password to a cybercriminal. With this information, they now have everything they need to infiltrate your systems. If you have MFA, the attack will fail unless the criminal is also able to physically steal that user's smartphone which would take significantly more work and reduces the likelihood your network will become compromised.

What Are My Next Steps?

While even the best cybersecurity protocols cannot prevent every situation, enabling MFA has become critically important to stay resilient from cyber threats and is one of many best practices, in addition to regularly testing and securing backups, remote access management, and periodic employee training on social engineering and business email compromise. If you think your organization lacks proper coverage, you're not alone. Our Holmes Murphy team can guide you to additional resources to make sure your cyber risk management program is comprehensive around prevention, mitigation, and financial protections.

- **Enable MFA:** Collaborate with your organization's leadership and IT department to determine the best course of action to implement MFA for remote, local, and privileged access.
- **Engage Cybersecurity Specialists:** If you need guidance selecting the right third-party cybersecurity service provider, Holmes Murphy has a proven network of vendors and can help you get connected.
- **Secure Insurance:** More than ever, now is the time to make sure you have a robust and up-to-date cyber insurance policy. Remember, many cyber insurance policies may offer you free expert consultations, discounted software services, and other risk reduction tools at no additional cost.

CONTACT US

Contact our Holmes Murphy specialists to Avoid, Reduce and Transfer your Cyber Risk and be better tomorrow than yesterday.

UNDERSTANDING ART

MONICA MINKEL
VP, Executive Risk Enterprise Leader
mminkel@holmesmurphy.com
(720) 622.8253

ROSS INGERSOLL
Executive Risk & Cyber Account Executive
ringersoll@holmesmurphy.com
(515) 381.7410

HOLMES MURPHY
INNOVATIVE CAPTIVE STRATEGIES
CREATIVE RISK SOLUTIONS
ACAP HealthWorks
avant SPECIALTY BENEFITS
charlesworth consulting
CSDZ A HOLMES MURPHY COMPANY
GCM Global Captive Management, Ltd.
ethos enhance. empower. engage.