NIST Small Business Cybersecurity Fact Sheet

Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

Passwords alone are not effective in securing your most sensitive business assets, as they have become too easy for threat actors to access. MFA is an important security enhancement that requires a user to verify their identity by providing more than just a username and password. It requires a user to provide a combination of two or more of the following:

- something you know (like a password or PIN)
- something you have (like a smart card or security key)
- something you are (like your fingerprint or face)

Protecting Your Business from a Common Cyber Threat: Phishing

Due to their effectiveness and simplicity to carry out, phishing attacks have rapidly become the tool of choice for cyber criminals. But what is phishing? Phishing refers to a variety of attacks that are intended to convince you to hand over sensitive information to an imposter. These attacks can come in many forms—most commonly in the form of a convincing email, text message, or social media message. What are they seeking? They're looking for financial gain and your account credentials, such as your password, pin, or one-time passcodes.

How does MFA Protect My Business From this Threat?

If a password is compromised, MFA creates a second barrier that makes it much hard for the threat actor to access your systems and data.

Example: Unfortunately, you received a convincing phishing email from what you thought was your accounting software provider. You entered your credentials into the fake website, giving the imposter your username and password. Thankfully, you have MFA enabled on this account. In addition to a username and password, a user also needs a security key to be granted access. Because the criminal did not have access to this security key, you were able to avert the crisis.

Visit the NIST Small Business Cybersecurity Corner:
https://www.nist.gov/itl/smallbusinesscyber

NIST Small Business Cybersecurity Fact Sheet

Multi-Factor Authentication

NIST Small Business Cybersecurity Corner

Taking MFA to the Next Level: Phishing-Resistant Authentication

Enabling MFA on all accounts that offer it is essential for reducing the cybersecurity risks to your business. However, some forms of MFA are more secure than others– as some forms of MFA can be susceptible to phishing threats such as One Time Pins (OTPs) and SMS based codes.

- FIDO authenticators paired with W3C's Web Authentication API are the most common form of phishing resistant authenticators widely available today. These can take the form of separate hardware keys or be embedded directly into platforms (for example your phone or laptop). Availability, practicality, and security of these "platform authenticators" increasingly puts strong, phishing resistant authenticators into user's hands without the need for additional devices or dongles.
- Not every transaction requires phishing resistant authentication. However, for applications that protect sensitive information (such as health information or PII data) or for users that have elevated privileges (such as admins or security personnel) organizations should be enforcing, or at least offering, phishing resistant authenticators.
- Individuals should explore the security settings for their more sensitive online accounts to see if phishing resistant authenticators are available and make use of them if they are. These tools are often easier, faster, and more convenient than the MFA – such as SMS text codes – they may currently be using.

Learn more here: https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

Questions to Consider

? Have we completed an inventory of all our systems to determine which ones offer multi-factor authentication?
? Have we enabled MFA on our most sensitive accounts? Are phishing resistant options available to us for use on our most sensitive applications?
? Do employees understand how to enable MFA and its importance in protecting the business?
? Do we have a policy for requiring use of MFA and phishing resistant MFA?
? Beyond MFA, are we considering other ways to manage access to our systems and data, such as:
  - Access to systems and data is limited to only those who need it to do their jobs.
  - Access is removed when needs change or when employees leave the business.
  - Administrative privileges to systems and devices are limited to only certain employees.
  - Using a password manager to create and store strong passwords.

Technical Deep Dive

- NIST SP 800-63 Digital Identity Guidelines
- NIST Identity and Access Management

Related Resources

- Cybersecurity and Infrastructure Security Agency (CISA) More than a Password

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE