A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A password-cracking expert has
easiest to remember because words can be easier to
recall than an acronym or series of numbers.

Options. Understand the security features
who offers MFA for your best protection.

MFA protects against phishing, social engineering and password brute-forces.

WORMS&ANTSEATPICNICS@7

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.

Password Security
Do's and Don'ts

PASSPHRASE EXAMPLES:
PASSPHRASE DON'TS:

A strong password is as lengthy as possible and
Complex:
Includes uppercase letters, lowercase letters, numbers, and
special characters.

Unique:
Use a different password for every account. Otherwise, a
single data breach can compromise
and Password Security
Multi-factor Authentication
What is Multi-Factor Authentication?
You understand this saying by now. A single line of defense - whether it is a password, a username and a password, or a password manager - is never enough in these days of increasing threats. Even if a bad actor knows your password, this added layer (multi factor authentication) would stop them from being able to access your assets.

Why should I care about MFA?
More and more entities are adding MFA - or multi-factor authentication - to strengthen the defenses of their users and their assets. With MFA, you are not just required to provide a single item of knowledge about yourself (e.g. your password). In many cases, MFA prompts you to provide two or more items of knowledge (e.g. a password and a second factor that might be a fingerprint or a Yubikey). This does not eliminate your password - there is added layer(s) of protection, that confirm you are who you say you are. Most MFA allows you to choose how to perform a multi-factor authentication - a quick single click or touch.