

Dear All,

While we are working from home during unprecedented time, It is important to think about protecting your password and make your data safe. We Administration team would request everyone to reset their respected login name and password for securing valuable data (Personal / Professional)

Reason to share this Information:

According to Thytotic, 80% of all cyber security attacks involve a weak or stolen password. Changing your password regularly reduces your risk of exposure and avoids a number of dangers.

Benefits of Changing Your Password Regularly

WHY?

1. Limits breaches to multiple accounts

Reusing your school email id password outside of school domain network, increases risk of access to several accounts if your password is hacked. Change your password to something unique for each of your accounts.

2. Prevents constant access

A hacker may try to access your account more than once over a period of time. Changing your password reduces the risk that they will have frequent access.

3. Prevents use of saved passwords

If you lose or change computers, it is possible someone may gain access to your saved passwords. Consistently changing your password means that even if someone finds an old, saved password, it will no longer be useful.

4. Limits access gained by keystroke loggers

A keystroke logger is surveillance technology used to record keystrokes. It is often used to steal login credentials. Regularly changing your password makes it less likely that passwords obtained this way will be useful for any length of time.

Credential stealing is more and more common, and is prevalent throughout the world.

Help keep your credentials safe by changing your password on a regular basis.

Guidelines for Password Management

Purpose

The purpose of this Guideline is to educate The Mindcrest School entire staff on the characteristics of a Strong Password as well as to provide recommendations on how to securely maintain and manage passwords.

Applies To

This Guideline applies to all staff that have a username and password to at least The Mindcrest School email id or application, independent of whether you are an end user or a senior's team.

Definitions

A Strong Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

The following are general recommendations for creating a Strong Password:

A Strong Password should -

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#\$%^&*()_-=)

A Strong Password should not -

- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.

The following are several recommendations for maintaining a Strong Password:

Do not share your password with anyone for any reason

Passwords should not be shared with anyone, including any students, faculty or staff. In situations where someone requires access to another individual's protected resources, For example, One Staff member need to share some data with another but he /she do not have access to proper internet or media so they share their login details with the other team mate. This type of solution is not encouraged. Passwords should not be shared even for the purpose of computer repair(Outside school premises) An alternative to doing this is to create a new account(After proper approval from Administrator) with an appropriate level of access for the repair person (Outside school Premises)

Do not write your password down or store it in an insecure manner

As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed.

Avoid reusing a password

When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

Avoid using the same password for multiple accounts

While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more

sensitive accounts such as your Social account or your online banking account. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.

Do not use automatic logon functionality

Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

Change default account passwords after received from IT team.

Default accounts are often the source of unauthorized access by a malicious user. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration of the system or application.

Below process we are using to protect our entire domain (Administrative Part)

Implement strict controls for system-level and shared service account passwords one hand managed.

We Do not use the same password for multiple administrator accounts

Using the same password for multiple accounts can simplify administration of systems and applications. However, this practice can also have a chain effect allowing an attacker to break into multiple systems as a result of compromising a single account password.

We Do not allow passwords to be transmitted in plain-text

Passwords transmitted in plain-text can be easily intercepted by someone with malicious intent. Protocols such as FTP, HTTP, SMTP and Telnet all natively transmit data (including your password) in plain-text. Secure alternatives include transmitting passwords via an encrypted tunnel (e.g. IPSec, SSH or SSL), using a one-way hash or implementing a ticket based authentication scheme such as Kerberos.

Implement automated notification of a password change or reset (We following below method to reset password with help of our info team)

A user's identity should always be validated prior to resetting a password. If the request is in-person, If the request is by phone, validating an identity is much more difficult. One method of doing this is to request a person to send email using Alternative email id to our info desk. Another option is to have the coordinator or class teacher email and confirm the request with respected authority. For obvious reasons, this would not work for student requests.

Below are some simple dos and don'ts:

1. Do avoid downloading attachments whenever possible (particularly if they offer information about stimulus checks or COVID-19 — that information can always be found on the relevant government websites).

2. Don't click on a link until hovering your cursor over it and confirming that it leads to a legitimate website.
3. Do use strong passwords.
4. Don't publicly post sensitive information.
5. Do download and install system/app updates on your devices (as they include important security patches)
6. Do treat suspicious links sent via text with just as much caution as links in your email inbox or anywhere else.