MARIST

Cybersecurity Best Practices

With so much of our daily lives connected to the Internet, it's important to remain safe and secure.

Below are guidelines that you should follow to remain secure:

Be cautious when it comes to email

Everyone has an email, whether it be for personal use (Gmail, Outlook, Yahoo, etc.) or work/ school (eg. Marist). Phishing is one of the most common cyber attacks. It is important to:

- Verify the senders of emails you receive. Bad actors can and will mask their sender address to look like someone or something trustworthy.
- Verify the links within an email to ensure they go to legitimate websites and services. Bad actors can and will create legitimate looking URLs and websites to lure people in.
- Verify attachments are from a trustworthy source before opening them.
- Never respond to suspicious looking emails and simply delete them.
- Never send non-password protected sensitive data over email.

Never share multi-factor authentication codes

Your Duo, ReACT, Microsoft Authenticator, etc. codes are the last line of defense if your username and password are compromised. Never share these codes with anyone under any circumstance. No office at Marist will ever ask for your MFA codes over text message, phone call, or email. In some scenarios, Help Desk will ask for emailed challenge codes or your ReACT security questions to verify your identity.

Sign-off of public devices

Marist has numerous computer labs and printing (WEPA) stations across campus. It is important to keep your account secure by always logging off after using publicly accessible devices on campus. To do this for:

- Workstations - Click the Windows icon in the bottom left, click the power icon, click restart.
- Printing stations - Click the logout button in the top right corner of the WEPA station.

Regularly update your devices

Ensure that your devices are updated in a timely manner. Sometimes, updates are released to address critical issues with a device that if left unchecked, could lead to a major security breach of the device. Also ensure that all applications/software are up to date as well.

Keep good password hygiene

Passwords are the best way to secure your accounts. Ensure that you do not reuse passwords for multiple accounts, as if one password gets compromised, all of your accounts are compromised. Make sure you do not use easily guessed passwords such as password123! or any passwords containing personal information which can also be easily accessible through social media.

Avoid open/unprotected/unencrypted Wi-Fi networks

Public wi-fi networks are a security risk. If the network is not encrypted, anyone can potenially access any data you transmit or receive. If your device is vulnerable to an attack, it may be possible for someone to access it remotely. Only join trusted networks - data encryption should be enabled on any network you trust.

Be aware of your social media presence

Be aware of what you share on the Internet via social media platforms. While posting personal information may seem harmless, bad actors can use this information to make inferences about you. These inferences can be used to socially engineer you through the use of phishing, smishing, etc. They can also be used to guess usernames and passwords. An example of this would be posting something with your pet's name and using a password that includes their name.

Use a secure password manager application

Password managers allow users to create and securely store passwords for multiple accounts and are protected by a Master Security Code or Passphrase. Downloading and installing a password manager application on your devices will allow for easy and secure access to account credentials. With this application, you only need to remember one password in order to access all other passwords.

Avoid using public USB charging stations

It’s better to use a charging adapter in a regular outlet rather than a USB charger in a public place. While it’s very uncommon, it is possible for a bad actor to connect a device on the other side of the wall jack and tamper with your device.

Immediately Report lost or stolen devices

Any lost or stolen device should be reported immediately to campus security and IT Department. IT will then attempt to delete the device information to prevent compromise of Marist College or personal data. For Marist issued devices, the IT Department will contact the wireless service provider to deactivate the cellular device capabilities to minimize unauthorized use.

Perform hard reset/wipe device before turning in/transferring device

Before any device is retired or transferred the device must be restored to “Factory Defaults”. This can be accomplished by performing a hard reset/wipe on device before turning in. IT can be contacted if assistance is needed in resetting device.

Avoid storing credentials in apps

Do not store your credentials directly in your mobile browser and applications. Use a secure password manager application to do so.

Be sure to check out our Cybersecurity Bookmark! Available at the Help Desk and WEPA printing stations across campus NOW! --->

MARIST
CYBERSECURITY

Go to the following link or scan QR Code:
marist.edu/information-security

TIPS

1. Don’t share your two-factor authentication codes (Duo, Authenticator etc.) with anybody.
2. Be careful about using public USB charging stations (Airports, etc.).
3. In computer labs, restart the computer when they aren’t in use & don’t enable “Keep me Signed In”.
4. Make sure your sensitive information is encrypted.
5. Don’t use the same password for multiple accounts.
6. Don’t log into financial accounts on public devices or on public WiFi.
7. Don’t scan random QR codes or click on random links.
8. Be safe on social media and watch what you share to the Internet.
9. Don’t join random WiFi Networks.
10. Marist Support, including offices, will never ask for your password.
11. Always keep your devices up-to-date: computer, phone, IoT, etc., and Anti-Virus.
12. Don’t fall for phishing!

For more details on these cyber tips
visit our site:
marist.edu/information-security
Any questions contact: Cybersecurity
cybersecurity@marist.edu

For more content from Marist Cybersecurity, visit:

marist.edu/information-security