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

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

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

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

MARIST

CYBERSECURITY

Phishing Email Examples:

You've heard of Phishing when it comes to cybersecurity, but have you heard of a similar tactic called Quishing? This is along the same lines as phishing but utilizes a QR code which when scanned will redirect users to a phishing site rather than a URL.

Why would attackers use QR codes over URLs?

- Quishing is less common than traditional phishing and thus target users have not experienced it as much, making it more likely that they fall for this method of attack.
- Mobile devices are required to scan QR codes and often do not have as strong protection as computers.
- QR codes are an embedded image on an email and are harder to detect by email protection tools.

Signs of Malicious QR codes

- Emails from unfamiliar senders.
- Spelling or grammatical errors.
- Little to no information surrounding physical QR codes in public.
- QR codes redirecting to login pages with unrecognized URLs.

For more details go to:
marist.edu/gonephishing

Report Phishing to:
phishing@marist.edu

MARIST

CYBERSECURITY

Phishing Email Examples:

You've heard of Phishing when it comes to cybersecurity, but have you heard of a similar tactic called Quishing? This is along the same lines as phishing but utilizes a QR code which when scanned will redirect users to a phishing site rather than a URL.

Why would attackers use QR codes over URLs?

- Quishing is less common than traditional phishing and thus target users have not experienced it as much, making it more likely that they fall for this method of attack.
- Mobile devices are required to scan QR codes and often do not have as strong protection as computers.
- QR codes are an embedded image on an email and are harder to detect by email protection tools.

Signs of Malicious QR codes

- Emails from unfamiliar senders.
- Spelling or grammatical errors.
- Little to no information surrounding physical QR codes in public.
- QR codes redirecting to login pages with unrecognized URLs.

For more details go to:
marist.edu/gonephishing

Report Phishing to:
phishing@marist.edu

MARIST

CYBERSECURITY

Phishing Email Examples:

You've heard of Phishing when it comes to cybersecurity, but have you heard of a similar tactic called Quishing? This is along the same lines as phishing but utilizes a QR code which when scanned will redirect users to a phishing site rather than a URL.

Why would attackers use QR codes over URLs?

- Quishing is less common than traditional phishing and thus target users have not experienced it as much, making it more likely that they fall for this method of attack.
- Mobile devices are required to scan QR codes and often do not have as strong protection as computers.
- QR codes are an embedded image on an email and are harder to detect by email protection tools.

Signs of Malicious QR codes

- Emails from unfamiliar senders.
- Spelling or grammatical errors.
- Little to no information surrounding physical QR codes in public.
- QR codes redirecting to login pages with unrecognized URLs.

For more details go to:
marist.edu/gonephishing

Report Phishing to:
phishing@marist.edu

MARIST

CYBERSECURITY

Phishing Email Examples:

You've heard of Phishing when it comes to cybersecurity, but have you heard of a similar tactic called Quishing? This is along the same lines as phishing but utilizes a QR code which when scanned will redirect users to a phishing site rather than a URL.

Why would attackers use QR codes over URLs?

- Quishing is less common than traditional phishing and thus target users have not experienced it as much, making it more likely that they fall for this method of attack.
- Mobile devices are required to scan QR codes and often do not have as strong protection as computers.
- QR codes are an embedded image on an email and are harder to detect by email protection tools.

Signs of Malicious QR codes

- Emails from unfamiliar senders.
- Spelling or grammatical errors.
- Little to no information surrounding physical QR codes in public.
- QR codes redirecting to login pages with unrecognized URLs.

For more details go to:
marist.edu/gonephishing

Report Phishing to:
phishing@marist.edu