BEST WAYS TO STAY **CYBER SAFE**
YOUR DATA, YOUR SECURITY

Recognize and Report Phishing

Phishing is a social-engineering attack where an adversary attempts to trick people into revealing sensitive information or performing actions that compromise security (clicking malicious links, opening infected attachments, transferring funds, or revealing credentials). Phishing can target individuals (spear-phishing), groups, or entire organizations.

How can you tell if a message is phishing?

- A tone that's urgent or makes you scared
- Sender email address doesn't match the company it's coming from
- Requests to send personal info
- Unexpected communications such as an email or attachment you weren't expecting
- Misspelled words, bad grammar, and odd URLs

Phishing Types

- Email
- Spear-phishing
- Whaling
- Smishing
- Vishing
- Clone Phishing
- Business Email Compromise (BEC)
- Credential Harvesting Sites
- Malicious Attachments

Do

- Verify email is real by calling the sender directly
- Report it to your IT!
- DELETE IT!

Don't

- Don't click links or even "unsubscribe" (just delete).
- Don't click unexpected or unrecognized attachment(s).
- Don't send or share personal info online or over the phone.

Cyber Security is not just a checklist,
it's a **culture**

Contact Us

security@cnmi.gov
https://finance.gov.mp
https://helpdesk.oit.cnmi.gov

Report an Incident to CISA

Use the online form at: cisa.gov/report

October 2025