Milima
Security

Phishing Attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message

How to Fight the Phish

'Fight the Phish' is a phishing awareness campaign designed to keep our community safe. We've created materials to help you identify, report, and avoid these types of attacks.

You are the first line of defense for protecting yourself and the campus community, here are simple tips to make sure you stay alert. Identify a phishing attack.

Keep your guard up.

SUBJECT: URGENT!!

Emails that create urgency and fear are usually fake. Scammers may insist that immediate action is necessary and pretend to be a friend, colleague, or another trusted entity. Don't let these tactics trick you into letting down your guard; stay calm and read the email carefully.

Phishing attacks can also occur through phone calls, texts, or instant messaging, so be aware of these other methods. It's important to be vigilant at all times and remain suspicious of sources that ask you for credentials and other personal information.

Your Responsibility

- Check the security of websites where you enter sensitive data and make sure they begin with “https://”. Some browsers will display padlock symbols in the address bar.

- Protect your credentials. If a person is asking you for sensitive information don't be afraid to ask why; no reputable company will ask for sensitive information via email, text message, or phone.
- Beware of attachments and links. E-mail attachments and links are commonly used to send malicious software. When you get a message with an attachment, or link, verify that it is legitimate - before clicking.

Float or Hover to reveal URL.

- Since emails can be easily spoofed, it’s a good habit to “float” your cursor over an address before replying. It's tempting, but don’t click on links or automatically reply to emails, even if it seems to be from someone you know. Instead, hover over the link with your mouse to see the underlying email or URL destination.

- For iOS touchscreen devices, press and hold the email address or link—don't tap it—to reveal the actual email address or URL. Remember, never reply to an unverified email or click on a link unless it goes to an entity or site that you trust.

Watch out for when it gets urgently personal.

"I can’t talk right now, but I need your help..."

- Attackers use personal, public information about you to lure you into responding. While masquerading as a colleague or university official, they try to get you to send them sensitive information, purchase gift cards, or get you to click on a malicious link to infect your computer or get access to an organization/university system.
- Always remember that organizations that care about protecting your information will never ask you to send bank account numbers, Social Security numbers, driver's license numbers, health information, or health insurance information via email.

To learn more about how to limit your digital footprint, visit Milima Security HERE

Report a phishing attack.

Send an alert/ message to info@milimatechnologies.com