MINNESOTA

PHISHING

PHISHING ATTACKS

Cybercriminals often use deceptive emails, social media posts, phone calls, and text messages to trick people into providing confidential or personal information for fraudulent purposes.

These phishing attacks can arrive as an email, a phone call, or a text message with fake audio or video impersonating trusted people or companies.

Learn the cyber skills needed to spot phishing attacks and to protect yourself, your family, your work, and sensitive information from cybercriminals.

ATTACK STRATEGIES

Impersonation

Pretending to be a trusted person or organization.

Urgency or threat

A deadline, emergency, locked account, or pay now.

Offer or prize

A great deal, an inheritance, or online-only relationship.

Request

Sensitive data demands for Social Security or account numbers or payments.

WHAT CYBER CRIMINALS WANT
AND WHAT YOU SHOULD DO

Passwords
Never provide login credentials.

Sensitive data
Don't share private information.

Infected devices
Don't click on unknown links.

Financial gain
Don't provide financial data or gift/credit card numbers.

ACTION STEPS

Stop and question it

- Pause and check the content.
- Identify whether the source is known and trusted.

Examine it

- Check the sender address and link/attachments.
- Look for the use of attack strategies.

Don't respond

- Don't click on links or open attachments.
- Don't provide passwords or sensitive/financial data.

Make contact

- Contact the source directly to confirm content.
- Use a safe word with family and friends to verify identity.

Report it

- Report suspicious emails to the email platform.
- Report fraud, scams, or identity theft to the Federal Trade Commission at ftc.gov.