HOW YOU CAN STOP HACKERS

Never provide personal identifiable information, including your Social Security Number, account numbers, login number, passwords, or birthdate. This is especially true when you did not initiate the conversation.

Never click on the link provided in an email unless you were expecting the email from a trusted associate.

If you believe the contact is legitimate, go to the company's website by directly typing the site address into your search engine.

Do not be intimidated by an email or caller who threatens dire consequences if you do not immediately provide or verify information. Legitimate contacts will not try to intimidate or scare you into complying with their demands.

If you fall victim to the attack, act immediately. Alert your manager and the OLIS service desk. Scam artists work hard to trick you, and you shouldn't be afraid to report an attack.

If you *see* something *say* something.

(406) 444-0912
OLIS-ServiceDesk@mt.gov

Montana Legislative Services Division
Office of Legislative Information Services

olis

June 2018

PHISHING & EMAIL SCAMS

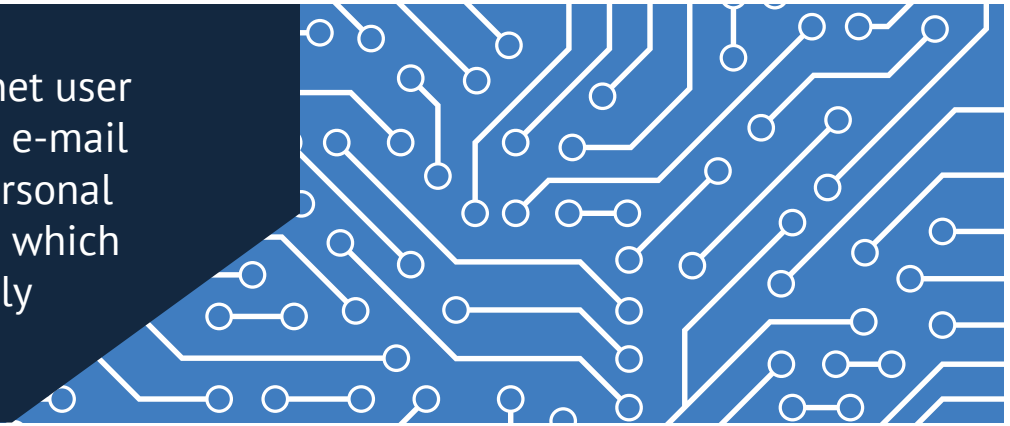
Recognize.
Prevent.
Mitigate.

olis MONTANA OFFICE OF LEGISLATIVE INFORMATION SERVICES

phish

verb | phish | \ fish \

: a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly



HOW PHISHING WORKS

A typical case:

- You receive an email from a reputable and familiar company or department. You may even have recently done business with them.
- The email requires immediate and unexpected action. "Please contact us immediately regarding your account."
- Remember, OLIS will not ask for your password or private information like a Social Security Number.
- The email then urges you to click on a button or go to a website. Or, it will ask you to open a Word document, PDF, or spreadsheet to verify information. Do not open suspicious attachments. Instead, contact OLIS.
- In a phishing attack, the website looks identical to what you expect. Do not enter your password from a link you received in an email.

HOW TO PROTECT YOURSELF

Do not provide personal information to anyone in an email or over the phone.

If you believe the contact may not be legitimate, **contact OLIS**. Do not forward or delete the email.

Never give out your password.

Tell OLIS if you think you may have opened a phishing attachment or given out sensitive information.

WHAT DO I DO IF I'M A VICTIM?

- If you opened an attachment that you think might be suspicious, turn off your machine. This helps prevent the spread of viruses and the continuation of back door access. Contact OLIS as soon as possible so they can get you up and running again.
- If you disclosed sensitive information in a phishing attack, contact OLIS and your manager immediately upon realizing this mistake. Don't be embarrassed or scared.
- Report all suspicious contacts and emails to OLIS whether you fell victim to them or not. We need to know how the attacks happen so we can effectively warn other employees.

Don't Hesitate.