Phishing Scams

E-mail scams and "phishing" are attempts to trick consumers into disclosing their personal or financial information. While online banking and e-commerce are generally safe, as a rule you should be very careful about giving out your personal financial information over the Internet.

Fake websites instruct consumers to "reenter" their credit card numbers, Social Security numbers, bank PINs or other personal information. If consumers provide the information requested, the data goes straight to the scammers, not to the legitimate company.

How to spot a phishing e-mail

Always be suspicious of any urgent, unsolicited e-mail that requests your personal financial information.

Typically, phishing e-mails:

- appear to come from companies with whom consumers may regularly do business.
- include unsettling or exciting (but untrue) statements. They may even threaten to close an account unless consumers act immediately.
- contain links to look-alike or "spoof" websites that use the legitimate company's trademarked logos and images. They might include features you see on secure sites, like an address that begins with "https://" and the yellow lock symbol.

Don't click on the link

Don't use the links in an e-mail, instant message or chat to get to any web page. Instead, call the company, or log onto the website directly. Don't fill out forms in e-mail messages that ask for personal financial information.

Be cautious and aware online

Be aware of where you are going online:

- Ensure that your browser and security patches are up to date.
- Look at the "address bar" at the top of the browser, not just the pictures on a web page.
- Consider installing a web browser toolbar to help protect you from known spoof websites.
- Regularly log into and check your online accounts. And regularly check your bank, credit and debit card statements.

If anything is suspicious or you don't recognize a transaction, immediately contact your bank and/or the card issuer.

How to report a phishing e-mail

When reporting spoofed messages, always include the entire original e-mail with its original header information intact. To report phishing e-mails, forward them to:

- reportphishing@antiphishing.org
- Federal Trade Commission at spam@uce.gov
- the legitimate company that was spoofed. Many larger companies have e-mail addresses specifically for phishing reports (e.g. spoof@eBay.com)

You can also report them to the FBI's Internet Crime Complaint Center at www.ic3.gov.

Your rights.
Your privacy.
Your peace of mind.

Montana Office of Consumer Protection
www.dojmt.gov/consumer
(406) 444-4500 • (800) 481-6896