

**Telephone phishing attacks are on the rise as well.** Often, these calls come in the form of an individual pretending to be from a tech company, most often Microsoft, and reporting to you that they have detected malware running on your computer. They then offer to help and attempt to manipulate the user to create a remote connection with them to remediate the problem. Doing so allows the attacker to gain access to the system, install malware and keyloggers, and potentially steal other important data. Microsoft will never legitimately contact a user to address malware infections, nor any other 3<sup>rd</sup>-party technology company.

Other telephone phishing scams center around the use of “bullying” the victim into providing a payment to avoid litigation. These accusatory types of calls center around back-taxes, unpaid speeding tickets, or other legal fines, and attempt to extort credit card numbers or bank account information from their targets.

Another telephone phishing scam claims to be from your bank, credit card company, or other financial institutions. They tell you that your account has been compromised and ask for account information so they can resolve the issue for you. Remember that financial institutions will never ask for your account information over the phone.

On any of these types of calls, it is advisable to just hang-up.



Regardless of how convincing the person on the other end of the phone is, never provide any personally identifiable, account, or address information. If you have any questions or think the call may be legitimate, look up the contact information for whoever called you in your records and contact them directly. Do not call back a number provided by the original caller.

If you are unsure about the validity of any emails or phone calls, you should request help from your IT Security staff to help determine the legitimacy of the information.



<http://infosec.mt.gov>



**Information  
Systems  
Security  
Office**

# Phishing Attacks

In this ever-changing information age of social media and digital technology, we as public servants and employees of the State of Montana must be vigilant to guard against the continual barrage of attacks we encounter from cybercriminals. Despite all the resources and vigilant efforts we allocate to secure the State's network and assets, one malicious email or phone call from a cybercriminal can be catastrophic to an employee or our systems.



Cybercriminals may attempt to install malicious software or gain access to your personal information under false pretenses. Two common methods used by cybercriminals are through Phishing email or phone calls. Phishing is a term used to describe the process of an individual attempting to use social engineering to manipulate confidential information from an employee. Most often, this information revolves around access to network credentials such as user-ids, passwords, social security numbers, and banking information such as bank account numbers or credit card numbers, usually with the intent of committing some sort of fraud such as identity theft or gaining privileged access to an information system.

There has been an increase in reported phishing attempts to State of Montana employees in both the form of email and phone calls. One of the best ways to avoid being a victim of a phishing attempt is to validate the information from the sender. Examples:

- ◆ **Are you expecting a package to be delivered from UPS or FEDEX?**
- ◆ **Have you heard about an increase in mailbox sizing from your email administrators?**
- ◆ **Do you know the person or recognize the originating email address?**
- ◆ **Pay attention to spelling and grammar. Cybercriminals sometimes have poor spelling or grammar.**
- ◆ **Beware of links in email. If you see a link in a suspicious email message, don't click on it.**
- ◆ **Cybercriminals often use threats that your security has been compromised.**
- ◆ **Spoofing popular websites or companies. Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites.**
- ◆ **If it sounds too good to be true, it probably is.**

Remember, no parcel delivery service will send you an email regarding an undeliverable package, and in order to increase your inbox size, your IT staff does not need your user id and password to do so. That leads us to evaluating a suspicious email.

First, always review the sender's email address. Do you really believe that someone from some random university or business is going to contact you about

upgrading your inbox?

Not all emails are equal, though, and there are some that are incredibly convincing. If you receive an email regarding an offer from a vendor or retailer, best security practices suggest not clicking the link within the email. Instead, open your web browser and manually navigate to the vendor or retailer's site to validate the offer. Other means of verifying addresses on a link include hovering your mouse over the link to see where it points, as well as copying the link and using a site, such as URLVoid.com to check a website's reputation.

