Phishing/Email Scams

Phishing is the use of email and fraudulent web sites to trick people into disclosing personal financial or identity information, such as credit card or Social Security numbers, user names, passwords and addresses. Although most "phishes" come as email, phishing scams can also come in the form of text messages and phone calls.

An email message may look harmless. Posing as your credit card company, your bank, or even Minot State University, it alerts you to a problem with your account and urges you to respond immediately by clicking a web link and "verifying" or "updating" your account information. The email and the web site may appear official, with all the familiar logos and corporate phrases. But they're bait, presented to fool you into divulging your personal financial information.

Identity thieves send out billions of phish messages every month, according to media reports. The Anti-Phishing Working Group estimates that 5% of those who receive a phish message actually respond. Financial losses are difficult to measure, largely because victims are unable to attribute unauthorized charges to phish messages.

Spam filters provide some defense against phishers by intercepting their messages, but the target is elusive. ***The best defense is the individual user.*** Because things aren't always what they seem to be, you should be skeptical about many emails.

Q&A

What is personal identity information?
Any piece of information which can potentially be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual is considered personal identity information. In includes, but is not limited to, Social Security, driver's license and financial account numbers. It can also include user names and passwords, PIN numbers, street and email addresses, telephone numbers or biometric data (e.g., fingerprints, DNA).

Is it okay to give out personal identity information to the University via email?
No. Because it can be very difficult to identify counterfeit emails, it is important to remember that Minot State University will not ask you to disclose personal identity information via email. Scammers will sometimes pose as "the University email service" or "the campus technical or help desk service." Don't be fooled! If you are asked to disclose your Social Security Number, account information, login and password, or other identity information, don't do it.

When in doubt, contact the Help Desk at 701-858-4444 for assistance.

What happens if I do respond to a phishing attempt?
If IT Central staff logs any response by you to a known phishing address, you will have your login and password disabled. To enable access, you may need to watch a short educational video and/or discuss the implications with campus IT.

Is getting access to my Peoplesoft ID and password really that unsafe?
Yes. Someone with your ID and password now has access to your personal information in HR Self-Service, including your payroll statements, financial aid records, grades, home address and more. Someone can steal your identity, change your course schedule, alter your research, and gain access to other applications within your department or even your home computer.

How to Recognize Scams

Scam tactics are increasingly sophisticated and change rapidly. Even if a request looks genuine, be skeptical and look for these warning flags:

- The message is unsolicited and asks you to update, confirm or reveal personal identity information (e.g., full SSN, account numbers, Peoplesoft ID, passwords, protected health information).
- The message creates a sense of urgency.
- The message has an unusual From address or an unusual Reply-To address instead of a "@minotstateu.edu or @my.minotstateu.edu" address.
- The (malicious) web site URL does not match the name of the institution that it allegedly represents.
- The link in the pop-up doesn’t match the printed text.
- The message is not personalized. Valid messages from banks and other legitimate sources usually refer to you by name.
- There are grammatical errors.

Dos and Don'ts

- Do keep your Internet browser and operating system up-to-date with the latest security patches and updates.
- Do be wary of unsolicited messages. Even though you may recognize the name of the sender, scam artists sometimes use these tactics to get personal information from you. Never give out your Peoplesoft ID, password, credit card or social security number in response to an unsolicited request.
- Do validate that when you are aware of an account change, that you are connected to a certified, encrypted web site. Look for a closed padlock in the status bar at the bottom of your browser window and for "https:" rather than "http:" in the URL.
- Do adjust your spam filters to ward off unwanted spam.
- Do use common sense. If you have any doubts, don’t respond. Contact your Help Desk at 701-858-4444 to ask for advice.
- Don't click the link. Instead, phone the company or do an Internet search for the company’s true web address.
- Don’t use forms that are embedded in the body of an email (even if the form appears legitimate). Only provide information over the phone or on a secure Web site (look for a Web address that starts with https://, not just http:// and for a padlock icon in the corner of the browser window).

- Don't open email or attachments from unknown sources. Many viruses arrive as executable files that are harmless until you start running them. .jpg file attachments have recently become a new format for spreading viruses.

To Report Phishing or Spam

To report general phishing emails, go to www.antiphishing.org. To report phishing emails that appear to be from within the MSU campus, contact the Help Desk at 701-858-4444.