Phishing Information and Process **2-1-16**

Phishing, as defined by the Federal Trade Commission, is "when [I]nternet fraudsters impersonate a legitimate organization to trick you into giving out your personal information." Plymouth State University account holders are ever-increasingly targets for phishing email attacks, which are becoming more sophisticated – some using PSU images and even office names and/or departments. Universities are unfortunately targeted frequently because we are research sites, and because we embrace a culture of openness and collaboration.

Phishers try to get you to act quickly through false statements of urgency, such as "act now or your account will be deleted," or "you are out of storage space, please verify your account information." They need you to act before you have an opportunity to reason, question, and analyze the message.

Phishers want your credentials for various reasons. They may be looking to use your credentials to send unsolicited bulk email ("SPAM") to people inside or outside PSU. They may also be looking to gain access to data they believe you have access to – perhaps based on your role as it is labeled in PSU's online directory or some other source. This type of phishing, where a specific individual is targeted, is called spear phishing, and is one of the most dangerous types – a type that is unfortunately on the rise. PSU takes phishing very seriously, as the ramifications to PSU could be significant.

The PSU Help Desk, helpdesk@plymouth.edu and (603) 535-2929, is well versed and skilled in determining whether any particular email message is phishing or not, and is happy to help you assess the legitimacy of any questionable message you receive.

Recognizing Phishing

Here are some points to consider when deciding if an email message is legitimate. Do not rely on any single factor, and do understand that this is not a comprehensive list.

- False claims, warnings and threats, such as messages telling you to act or your account will be closed/locked, or that – ironically – your account has been compromised and you must reconfirm by clicking a link in the message. Or that you are over quota and your data will be deleted.

- Unofficial "From" addresses. PSU will only send messages from PSU accounts. However, know that a "From" address can be spoofed, and sometimes if one PSU account has been phished, that compromised PSU account may be used to try to phish other members of the PSU Community, because the address would have the appearance of legitimacy.

- Peculiar email greeting or closing. Phishers tend to use odd greetings and closings, because they are unfamiliar with the nomenclature we use at PSU. Instead of "The PSU Help Desk," a closing may be "The Service Desk" or "Your Service Team." A greeting may be "Dear valued xyz1010@plymouth.edu" instead of your name, because all the phisher may have access to is your email address.

- Grammar and spelling. Phishers – and cybercriminals in general – are not known for proficient grammar and spelling. When PSU sends a message, particularly a message going to a wide audience, we generally have multiple people read and proof the text before clicking "send." If you see mis-spelled words and grammatical mistakes, it should raise your suspicions.

- Web address ("URL"). Phishers want you to think you've clicked a legitimate URL, so they will try to construct one that appears real, so you may see a URL such as http://www.plymouth.edu.*phishingsite.us*/webapp/portal/passwords, instead of the legitimate site https://www.plymouth.edu/webapp/portal/passwords/. It is likely that "phishingsite.us," in the above example, has been exploited, and the phisher is in control of it.

- Spoofing PSU websites. Phishers will capture graphics from PSU's websites and use them in constructing their phishing websites, and they may include links that direct people to legitimate PSU websites, such as our main page, or the Help Desk. Inclusion of PSU graphics, unfortunately, is happening more frequently. These spoofs are recognizable by "mousing over" the links and seeing that they do not direct you to PSU websites and services.

The following websites have additional information and examples, and portions of them were used as guidelines and sources for the information above. They are each excellent resources.

Microsoft - "How to recognize phishing email messages, links, or phone calls"

Google - "Unwanted or suspicious mail"

Apple - "Identifying fraudulent 'phishing' email"

Yahoo - "How can I recognize a phishing email?"

PayPal - "Your Guide to Phishing"

Amazon - "This E-mail from Amazon?"

Wired - "Identify a Phishing Scam"

FBI - "Spear Phishers"

Protecting Yourself from Phishers

Be aware, be skeptical, and think before you click. If an email seems to be urging you to "act now" or "your account will be deleted," it is probably a phishing attempt.

Look carefully at the URL links included in the message. Do not trust those that you see in the message, but hover over the link with your pointer instead. Do these links look legitimate, or are they awkward?

Remember that PSU will *never* solicit a username or password via email under any circumstances, and any email to the contrary should immediately be considered suspect. Do not provide passwords or highly sensitive information in response to an email or phone call.

If you did not initiate contact with PSU ITS support (e.g. the PSU Help Desk), do not provide any personal information (e.g. phone number, username, ID number, password, etc.).

What to do if You Are Phished

- If you believe you were phished, change your password and contact the Help Desk immediately. They can take steps to help you find out what may have occurred as a result of the phishing, and they can use the message you received to proactively warn other members of our community.

- If PSU discovers you were phished, your account will be immediately locked in order to prevent further unauthorized access to your account. In a case where your account is locked because of phishing, PSU ITS will make its best efforts to contact the account holder promptly, and access to your account will be restored following a brief conversation, a password change, and you may be scheduled to attend a session on awareness of phishing and its consequences.

Further Reading about Phishing

National Cyber Security Alliance - "Spam and Phishing"

OnGuard Online - "Phishing"

Anti-Phishing Working Group - "How To Avoid Phishing Scams"

United States Computer Emergency Readiness Team (US-CERT) - "Avoiding Social Engineering and Phishing Attacks"

Phishing Quizzes

Do you want to see what phishing looks like? Try these quizzes:

OpenDNS - "Think you can outsmart Internet scammers?"

McAfee- "Put your phishing knowledge to the test"