Got Phished! Now What?

First, don't panic. You are not alone! Many people have fallen victim to phishers and have been tricked into giving away their passwords or personally identifiable information. Once you realize that you've been compromised, there are some immediate steps you should take to protect yourself, your information and your identity.

Steps to Securing Your Information after a Phishing Attack

- Step 1: Change your passwords
- Step 2: Check the email rules on your Syracuse University email
- Step 3: Verify MySlice information has not been altered
- Step 4: Notify the ITS Information Security department
- Step 5: Reduce threats to your identity
- Step 6: Minimize future threats
- Getting Help

Step 1: Change your passwords

You should immediately change your Syracuse University (NetID) password. Instructions for doing so can be found on the Answers "Password Change" page.

You should not be using the same password you use for your NetID anywhere else, but if you do, you should change those passwords to be *unique* passwords.

Step 2: Check the email rules on your Syracuse University email

Attackers may attempt to add email rules to your account in an attempt to hide their activity from you. They will set up rules to forward and/or delete email from key individuals or University offices such as 'ITS', 'Bursar" or 'Payroll'.

- Instructions for students to check their inbox rules can be found on the Answers "Securing SUMail Account After Security Lock" page.
- Faculty and Staff should contact the ITS Support Center or their local IT support staff.

Please take note of what those rules are and provide them to the Information Security Department.

Step 3: Verify MySlice information has not been altered

Attackers may attempt to change information related to your account including personal and financial information.

Users should verify the following information has not been altered:

- Names
- Addresses
- Any financial records (including verifying refund requests)
- Direct deposit (if applicable)

Step 4: Notify the ITS Information Security department

The ITS Information Security Department depends on the Syracuse University community to help detect and protect against phishing attacks. Taking a brief moment to send us an email may help protect many others from the attack. Simply forwarding the message to ITSecurity@listserv.syr.edu is helpful, but providing additional information as shown below will help us better protect other individuals and your access.

- **Have you already changed your password?** Letting us know that you've already changed your password may prevent us from locking your account if we detect your original password being compromised.
- **Provide the original email headers**. Headers contain detailed mail routing information that we can use to investigate the attack. Instructions on obtaining the headers can be found on the Answers "Sending Email Headers" page.
- **What information you provided**. Did you provide your SSN? Your date of birth? Your name? Your NetID/Password? We don't need the actual information, but letting us know the type of information you entered helps us to understand the scope of the attack.
- **The content of your inbox rules.** If you found malicious rules in your email box, letting us know what those were will help us detect other accounts that have been compromised.

Step 5: Reduce threats to your identity

- *IdentityTheft.gov* is the U.S. government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process. Get help to report and recover from identity theft at: https://www.identitytheft.gov/and https://identitytheft.gov/Info-Lost-or-Stolen
- Freeze your credit report to prevent attackers from obtaining credit histories and opening new lines of credit:https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
- Review the recommendations from the Social security Administration about identity theft and your SSN atwww.ssa.gov/pubs/10064.html
- Create your online Social Security account -- regardless of your age or retirement eligibility -- to prevent attackers from doing so: https://www.ssa.gov/myaccount/. If you already have an account, review your statements regularly and be alert for benefits activity you didn't initiate.

Step 6: Minimize future threats

- Enable two-factor authentication for your online accounts. This will protect you against unauthorized use of your credentials, even if they are stolen. For your University Office 365 , visit NetId.syr.edu and click *Two-factor Opt-in*.
- Be suspicious of any email from senders you don't know, or that seems out of character for the sender. Verify that the sender is actually who they appear to be before clicking on any links or attachments.
- Any request for money or goods is bound to be fraudulent. If it claims to be from a campus member, contact them or their office to verify first, or check with Information Security.
- Verify the URL of any link before you click it by hovering your cursor over the link and examining the URL. If you don't recognize the URL, don't click it.
- Never open attachments unless they are from someone you know or are otherwise expected.
- Delete any suspicious emails, before opening them if possible.
- Don't enter your username and password (especially your University NetID) to access any website if you are not 100% sure of its validity. In particular, you should be suspicious of email messages that have links to sites that ask you to use your University NetID and password to log in.
- Keep your computer software updated and patched, particularly your antivirus and anti-malware software.
- Make sure your computer's firewall is installed and running.
- Remember that nobody at Syracuse University will ever ask for your NetID or password for any reason, in any form other than when you're logging in to an SU system. If somebody does, they're not representing the University or any of its offices. Report any occurrences to itsecurity@syr.edu.

Getting Help

If you need more information or assistance with verifying any email messages, please do not hesitate to contact your local IT support team (if you're faculty or staff), or the ITS Service Center (if you're a student) at 315.443.2677 or help@syr.edu.

To receive timely notification from ITS of current information security threats follow SecurecUse Twitter and SecurecUse Facebook.

Top