



Beware of phishing scams (emails)



By Sharen Custer

Please note: Emails sent from xxxxx @ NYSSkillsUSA.org will never ask for your personal account information or demand payment.

Identity theft is on the rise. Unfortunately it's also a time when consumers need to be on the lookout for potential scams.

Phishing scams, in particular, tend to flourish every month, every day.... especially during the holidays. In this type of con, a scammer will send malicious emails and messages to consumers to try to obtain credit card details, usernames, passwords, and other sensitive information.

How to tell if you received a Phishing/Spam email from NYSSkillsUSA.org:

Pay close attention to the return email address, you can usually just run your mouse across the return email address and you will see it pointing to a different email address other than ours **.nysskillsusa.org**.

If you have questions or are not sure, **do not reply** to this email call one of our contacts on our site to verify. You can contact us directly if you need assistance, please don't hesitate to call anyone of our Staff Contacts. We take this very serious and understand your concern.

Pay close attention to the web link address. Scammers will often misspell words in a URL. Be on the lookout for extra letters, odd combinations, and extra affixes at the end of URLs. **Don't click links** in suspicious messages or emails. Sometimes all it takes for a phishing attack to be successful is for the recipient to click on a malicious link. In addition to misspelled words, phishing emails are often **riddled with other grammatical errors**. If the email does not look like something that was professionally edited, you could be looking at a scam.

