CORNING

Frequently Asked Questions
Multi-Factor Authentication for OptoCommerce® Account

Beginning March 31, Corning is integrating a leading multi-factor authentication software (Okta), into our OptoCommerce® platform to provide an extra layer of protection for your data. Multi-factor authentication not only provides secure connections between people and technology but also makes accessing OptoCommerce easier and more secure.

Q: What is Multi-Factor Authentication (MFA)?
A: Multi-Factor Authentication (MFA) is a security measure that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN. By requiring multiple forms of identification, MFA increases the difficulty for unauthorized users to gain access, providing a higher level of security.

Q: Why is MFA being implemented?
A: MFA is being implemented to enhance the security of our systems and protect sensitive information. It adds an extra layer of protection by requiring users to verify their identity through multiple methods, making it more difficult for unauthorized individuals to access our systems.

Q: How will MFA affect my login process?
A: On March 31, you will receive an email from noreply@okta.com prompting you to complete a one-time set-up of MFA. Following set-up, MFA will be required for all future logins. Learn more here.

Q: I do not see the email from noreply@okta.com. What do I do?
A: Check your spam or junk folder, as sometimes emails can be inadvertently directed there. If they still do not see an email from noreply@okta.com, please reach out to ceopto@corning.com.

Q: What is Okta?
A: Okta is a leading Multi-Factor Authentication software. Okta will be integrated into Corning's OptoCommerce platform to provide an extra layer of protection for your data.

Q: What verification methods are available for MFA?
A: The available verification methods for MFA include:

- Password (Required First Factor)
- Second Factors to choose from:
  - Email verification (Note: this option will be automatically selected at set-up)
  - SMS/Voice call verification
  - Google Authenticator code verification

Q: Do I need to set up multiple factors of authentication?

A: Email verification will automatically be selected as your second form of authentication. Once you have set up email as the second form of authentication, no additional action is required.

However, you have the option to select additional forms of authentication (e.g. SMS/voice call or Google Authenticator), if desired. Follow these instructions to complete one-time set up of your MFA.

Q: What happens if I lose access to my verification device?
A: If you lose access to your verification device (e.g., your phone), you can use a backup verification method if you have set one up. If you do not have a backup method, please reach out to ceopto@corning.com to request support.

.
Q: What happens if for some other reason I cannot login using MFA?
A: Please contact ceopto@corning.com to request support.

Please be assured that our dedicated customer support team is ready to assist you through this transition. If you have any questions, feel free to reach out to your Corning account manager or the Corning support team at ceopto@corning.com.