WineRe®
Specialty Property & Casualty Insurance Program

Cyber Risks in the Wine Industry: Phishing Attacks on the Rise

What is Phishing?
Phishing is a method used to compromise the computers of and steal sensitive information from individuals by pretending to be an email from or the website of a trusted organization.

A subset and highly effective form of phishing attack is a spear-phishing attack in which a hacker will research an intended target and include details in an email that makes the email seem more credible.

Phishing Techniques include:
- Embedding a link in an email that redirects your employee to an unsecure website that requests sensitive information.
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information.
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

How to Prepare
- Consider a Cyber Insurance Policy, which covers most costs associated with a breach.
- Maintain effective and current software to combat phishing.
- Educate employees and conduct training sessions on identifying suspected phishing emails.
- Maintain written and trained internal protocols around sensitive data and methods of account payables.

How to Detect
- Examine incoming email addresses closely.
- Review a request to determine if it is outside normal corporate protocol.
- When you receive links via email, if you want to access them, type the address in your Internet browser instead of clicking on them.
- When in doubt, pick up the phone and speak to a manager about the request.

How to Prevent
- Never submit confidential information via an embedded email ink or submission form.
- Never use embedded links in an email to connect to a website.
- Two Factor Authentication should be instituted across all sensitive data and accounting procedures.

Brendan Wright
John Sutak Risk Services
Brendan.Wright@johnsutakrisk.com
Ph: (415) 757-2520