Phishing is No April Fools' Day Fun: FTC Advice to Companies

When internet scammers mimic reputable businesses to trick consumers into giving their personal information, it doesn't just hurt the consumers, it hurts the good name of the companies they are impersonating. By taking preventive action and by offering immediate advice and support, companies can help stop phishing and retain customer goodwill. In March, the Federal Trade Commission offered advice on doing just that. It first released a study on how companies can prevent criminals from using their company domains in phishing scams. It then issued guidance and a video on how businesses should respond when they learn of phishing attacks using their company name or brand. In the FTC study, it recommends that businesses protect their domains from phishing scams by using methods such as:

- Domain level email authentication to allow receiving mail servers to verify that a message claiming to be from the business actually came from a domain authorized by the business; and
- Domain Message Authentication Reporting & Conformance, which, among other things:
  - Enables businesses to gather intelligence on how scam artists are misusing their domains; and
  - Instructs receiving email servers on how to treat unauthenticated messages that claim to be from a company's domain.

Plus, in the FTC guidance, it suggests that companies do the following when they learn their name or mark is being used in a phishing scam:

- **Notify consumers of the scam ASAP** – Use social media, email and other methods to immediately:
  - Inform your customers of the scam;
  - Warn them to ignore suspicious emails or texts appearing to be from you; and
  - Remind them that your company would never solicit sensitive personal information through insecure channels like email or text message.
- **Contact law enforcement** –
  - Report the scam to the FBI's Internet Crime Complaint Center; and
  - Encourage affected customers to forward phishing emails impersonating your business to the public-private partnership against cybercrime known as the Anti Phishing Working Group.
- **Provide resources for affected consumers** –
  - Direct affected consumers to www.IdentityTheft.gov where they can report and recover from identity theft; and
  - Provide them with resources to protect themselves such as the FTC's consumer information site.
- **Update your company's security practices to reflect latest available information** –
  - Review the FTC's data security portal for information on securing sensitive information;
  - Follow case developments and read publications designed for companies of any size or sector including Start with Security and the recently refreshed Protecting Personal Information: A Guide for Business.

These twin FTC pronouncements offer good advice for companies and may signal an FTC intent to take enforcement action in the future against companies that fail to take reasonable security measures to

protect against phishing scams. *This article is general in nature and does not constitute legal advice. Readers with legal questions should consult with an attorney prior to making any legal decisions.