Press Release:

FTC Staff study finds that many major online businesses are using email authentication, but few are using DMARC, which would provide additional phishing protection

In a study released today, the Federal Trade Commission's Office of Technology Research and Investigation (OTech) reports that most major online businesses are using proper email authentication technology to prevent phishing emails, but few of these businesses are taking full advantage of the latest technologies to combat phishing.

Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source such as an internet service provider, a bank, or a mortgage company. It asks the consumer to provide personal identifying information, and then the scammer uses the information to open new accounts or invade the consumer's existing accounts.

Specifically, the OTech study found that 86 percent of major online businesses it studied are using Sender Policy Framework (SPF), an email authentication technology that enables Internet Service Providers to determine whether messages that claim to be from the businesses' email addresses actually come from the businesses. Fewer than 10 percent of the businesses, however, have implemented a supplemental technology known as Domain Message Authentication Reporting & Conformance (DMARC) in a manner which would allow the businesses to receive intelligence on potential spoofing attempts and to instruct ISPs to automatically reject any unauthenticated messages that claimed to be from the businesses' email addresses. By using DMARC to instruct receiving ISPs to reject unauthenticated messages, online businesses could further combat phishing by keeping these scam emails from showing up in consumers' inboxes.

For a full analysis of the staff's findings, and to learn about its methodology, read the entire Staff Perspective or watch this video.

Report's Conclusion:

Our research shows that most top online businesses have adopted email authentication technologies, but only a small fraction have taken the additional step of implementing DMARC. With DMARC, a business can protect its domains from being used by phishers and other scammers by instructing receiving domains to automatically reject unauthenticated messages that claim to be from the business's domains. This powerful tool could be an effective means of combatting phishing scams. Unfortunately, our research demonstrates that few of the top US online businesses are using the DMARC solution to the fullest extent. Wider implementation of DMARC with the "p=reject" instruction could further combat phishing by keeping these scam emails from ever showing up in consumers' inboxes.