Barley Snyder

WARNING: Heightened alert for phishing scams amid GDPR transition

PUBLISHED ON
May 30, 2018

When there is something new, confusing, and much-hyped on the Internet, you can bet criminals are going to find a way to exploit it.

That is so far the case with the General Data Protection Regulation (GDPR), the data privacy rules for all individuals within the European Union (EU) and European Economic Area that went live Friday.

The primary aim of GDPR is to provide EU citizens and residents more control over their personal data. It is also intended to simplify the regulatory environment for international business by providing a comprehensive, yet uniform, set of regulations. While its aim is to simplify, however, GDPR has been presenting its fair share of problems, especially to U.S. businesses that are still battling with confusion and uncertainty of whether and how GDPR applies to them.

You may have noticed that amid the transition to the new requirements of GDPR, businesses around the world are scrambling to update their privacy notices. As they do, they are flooding our in-boxes, advising us of the changes made to their privacy policies in valid attempts to comply with GDPR. Unfortunately, however, we are now also seeing criminals exploiting this confusion. Industry experts and associations, including those in banking and financial services sectors, are reporting that criminals are now spoofing bank and other businesses with phishing scams relating to GDPR and attempting, at alarming rates, to persuade us to disclose our personal banking and other information.

The same advice applies in these circumstances as it does in all phishing scams. As Pennsylvania Attorney General Josh Shapiro suggests:

- Never reply to unsolicited e-mails or pop-up messages asking for personal or financial information or requests to "verify" data about your account. Banks, credit card companies, and businesses do not (and should not) send requests for PIN numbers or sensitive information to their customers.

- Do not call any phone numbers contained in messages purporting to be from your bank or other companies you do business with. Providing sensitive information to strangers by phone is as dangerous as sending it in an e-mail. Also, don't open any links or documents contained in these messages. They may route you to a bogus website or download a virus onto your computer.

If you have any questions about GDPR or other cybersecurity matters, pleasereach out to me.

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com