1/25/17

By Administrator

According to a new report from the Identity Theft Resource Center (ITRC) and CyberScout, the number of U.S data breaches tracked last year hit an all-time high of 1,013, a 40 percent increase over the 780 breaches reported in 2015. The ITRC, a nonprofit organization that provides free assistance for victims of identity theft and consumer education, has been tracking data breaches since 2005.

It's not clear how much of the increase is due to more breaches occurring; the fact that many state agencies are now making data breach notifications public on their websites and that the ITRC has been stepping up its efforts to get breach information through direct contact with offices of state attorneys general and Freedom of Information Act requests may be contributing factors. What is clear is that businesses continue to be the main target of identity thieves and that hacking/skimming/phishing attacks are the leading cause of data breach incidents.

Many of those attacks last year were CEO spear phishing efforts in which company employees are tricked into sending cybercriminals payroll and other sensitive personal data in response to emails that look like they're from their bosses. This information can be used to file fraudulent tax returns and commit other forms of identity theft. It's especially worrisome because while a compromised credit card account number can be changed, a stolen Social Security number cannot.

What should you do if you get a notice that your data has been breached? The Federal Trade Commission's video provides tips and directs you to the www.identitytheft.gov website to guide you through a recovery plan.

And what should you do if your company or organization experiences a breach? Consumer Federation of America answers 7 questions to ask if you are considering purchasing identity theft services to help those affected by the breach.