MediaWell

News Item

Email Hackers Are Winning | The Atlantic

By Quinn Norton
May 23, 2018
New security research on so-called “Efail” demonstrates that the most commonly-used encryption in email clients does not work, and that this has huge implications for our privacy.

> “Email is really dangerous,” says Green, “People don’t care about JavaScript in your browser or remote image access or even fancy encrypted email stuff because mostly the bad guys are phishing the CEO with straight HTML email from PayPal.EvilCompany.com and he goes for it.”
>
> Most hacks in the real world start this exact way: an email forged, telling you things that aren’t true, while acting like a web browser. If they want to look like a bank, they can load their images from a bank’s website. If the hacker wants you personally, they can send a mail from your coworker, spouse, or best friend, frantically asking you to check something on your calendar. When you try to log into that calendar, they have your login and password. Or in some cases, you don’t have to do anything to be in trouble. Code execution, or the ability to run a program on someone else’s computer, is often the most powerful attack, potentially letting someone else silently and invisibly take over your computer. Speaking of the Efail paper, Green says, “You could run JavaScript in … five corporate email clients and it was a footnote in this paper.” Such a thing, properly exploited by the sender of an email, could allow that sender access to the information stored on the receiver’s computer.

Source: Email Hackers Are Winning – The Atlantic