Snapchat, Seagate among companies duped in tax-fraud scam

March 9 2016, by Michael Liedtke And Sarah Skidmore Sell

In this Thursday, Oct. 24, 2013, file photo, Snapchat CEO Evan Spiegel poses for a photo in Los Angeles. Tax-filing season is turning into a nightmare for thousands of employees working at companies tricked into relinquishing tax documents exposing people's incomes, addresses and Social Security numbers to scam artists. In fact, in a Feb. 28, 2016, post on its corporate blog, Snapchat revealed that its payroll department had been duped by an email impersonating Spiegel. (AP Photo/Jae C. Hong, File)

Tax-filing season is turning into a nightmare for thousands of employees

whose companies have been duped by email fraudsters. A major phishing scheme has tricked several major companies—among them, the messaging service Snapchat and disk-drive maker Seagate Technology—into relinquishing tax documents that exposed their workers' incomes, addresses and Social Security numbers.

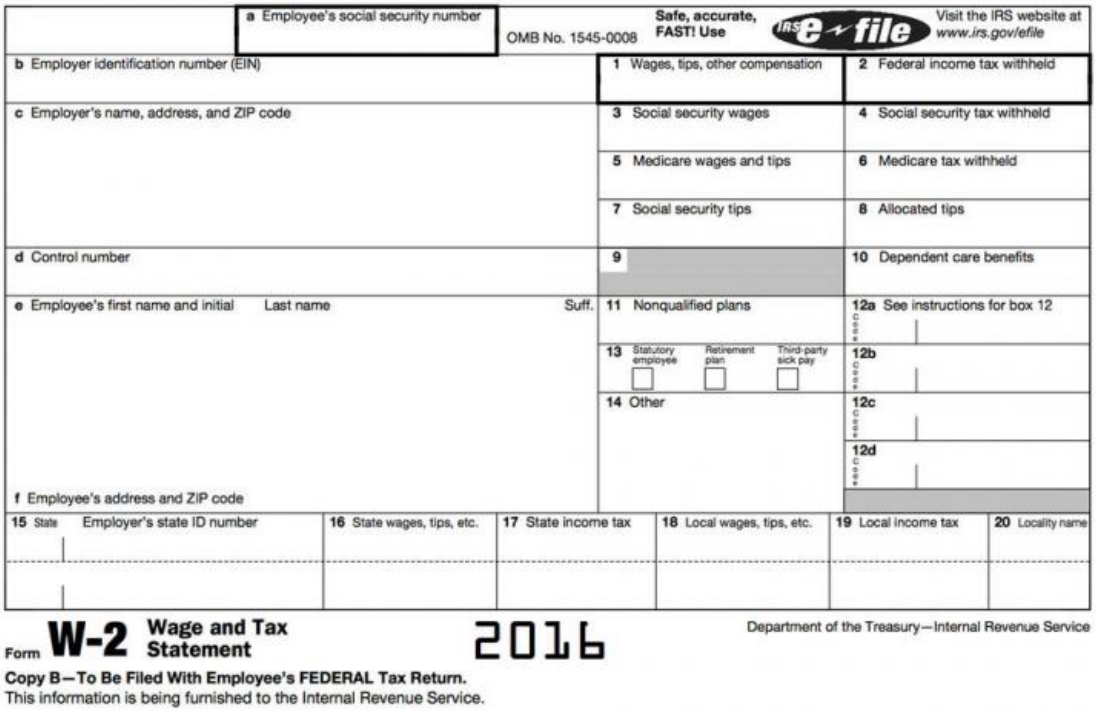
The scam, which involved fake emails purportedly sent by top company officials, convinced the companies involved to send out W-2 tax forms that are ideal for identity theft. For instance, W-2 data can easily be used to file bogus tax returns and claim fraudulent refunds.

The embarrassing breakdowns have prompted employers to apologize and offer free credit monitoring to employees. Such measures, however, won't necessarily shield unwitting victims from the headaches that typically follow identity theft.

"This mistake was caused by human error and lack of vigilance, and could have been prevented," Seagate's chief financial officer, Dave Morton, wrote in a March 4 email to the company's employees about the breach.

The swindlers behind the tax scam are exploiting human gullibility rather than weaknesses in computer or Internet security. They have targeted company payroll and personnel departments, in many instances with emails claiming to be requests from the company CEO asking for copies of worker W-2s.

The schemes are so widespread that the IRS sent a March 1 notice alerting employers' payroll departments of the spoofing emails. The IRS said it's seen a 400 percent increase in phishing and computer malware incidents this tax-filing season.



a Employee's social security number | OMB No. 1545-0008 | Safe, accurate, FAST! Use | Visit the IRS website at www.irs.gov/efile

b Employer identification number (EIN) | 1 Wages, tips, other compensation | 2 Federal income tax withheld

c Employer's name, address, and ZIP code | 3 Social security wages | 4 Social security tax withheld | 5 Medicare wages and tips | 6 Medicare tax withheld | 7 Social security tips | 8 Allocated tips

d Control number | 9 | 10 Dependent care benefits

e Employee's first name and initial | Last name | Suff. | 11 Nonqualified plans | 12a See instructions for box 12

13 Statutory employee | Retirement plan | Third-party sick pay | 12b

14 Other | 12c | 12d

f Employee's address and ZIP code

15 State	Employer's state ID number	16 State wages, tips, etc.	17 State income tax	18 Local wages, tips, etc.	19 Local income tax	20 Locality name

Form W-2 Wage and Tax Statement 2016 — Department of the Treasury—Internal Revenue Service

Copy B—To Be Filed With Employee's FEDERAL Tax Return.
This information is being furnished to the Internal Revenue Service.

This screen grab from the Internal Revenue Service website shows a sample W-2 form. Employers are being tricked into sending detailed employee tax information to scammers as part of an emerging tax fraud campaign. Two prominent technology firms, Seagate Technologies and Snapchat, are among recent victims. (IRS via AP)

The agency said the scheme has so far claimed "several victims," but declined to disclose how many other employers had reported releasing W-2s to unauthorized parties.

"It's premature to provide numbers at this point, but even one company being fooled by these criminals is too many," the IRS said in a statement.

The federal alert didn't come soon enough for Snapchat, which on Feb.

28 revealed that its payroll department had been duped by an email impersonating its CEO, Evan Spiegel. The Los Angeles company didn't specify how many employee W-2s it released. Snapchat didn't respond to requests for comment Tuesday.

"When something like this happens, all you can do is own up to your mistake, take care of the people affected, and learn from what went wrong," Snapchat wrote in a post on its corporate blog .

Seagate acknowledged surrendering the W-2s for all of its current and former employees who worked at the company last year. The Cupertino, California, company said "several thousand" people were affected, but declined to be more precise. As of July last year, Seagate employed about 52,000 workers but all but 10,500 of them were based in Asia.

Both Snapchat and Seagate notified federal authorities about the phishing attacks and are offering affected workers two years of free credit monitoring.

It's unclear how many other employers have been sucked into the tax scam. Hundreds of companies appear to have been targeted, according to Stu Sjouwerman, CEO of KnowBe4, a Florida company that trains employers to detect and avoid such scams.

Phishing attacks commonly occur during holidays and other annual events, such as tax season, to prey upon people's routines, said Fatih Orhan, director of technology at security firm Comodo. The attacks are becoming increasingly effective because they rely on powers of persuasion instead of an attachment or link that might raise suspicion, said Ed Jennings, chief operating officer at email security company Mimecast.

"It's just like someone who convinces you to hand over $20 on the

street," Jennings said.

Sjouwerman said the W-2 seeking attacks are most likely are being sent by Eastern European hacker groups planning to sell the information or claim fraudulent tax refunds.

The most effective phishing attacks use emails decked in company logos and colors to reduce the chances of detection, Orhan said. It's relatively easy for con artists to pose as a CEO online, since they can quickly fetch convincing details from a Google search or a perusal of professional networking service LinkedIn.

That doesn't excuse payroll or personnel departments who reflexively acquiesce to requests in apparently legitimate email, experts say. For instance, Sjouwerman said his firm's controller received a phishing email that, at first glance, appeared to be sent by him. But the email asked the controller to "kindly prepare" employees' W-2s, a phrase that he never uses. Company employees were alert enough not to send out the W-2s.

Even without a red flag like that, payroll and personnel specialists should be trained well enough to question why a CEO needs to see individual worker W-2s in the first place.

"It's a case of: 'Oh, the boss wants it'," Sjouwerman said. "They stop thinking, 'Why would this be?'"