TAX-TIME PHISHING SCAMS

How They Work and What to Do About Them

What is Tax-related Phishing?

Tax-related phishing occurs when cybercriminals, spoofing emails or impersonating co-workers, executives or authorities, send fraudulent emails to employees asking for tax information (W-2s and other employee documents) or requesting tax-related responses. When employees respond to these requests, they may inadvertently send private data to a criminal. In other cases, opening the email allows malicious software to launch, infiltrating a company's computer systems.

Who Typically Receives Tax-related Phishing Emails?

Employees who handle a company's tax matters

Human Resources Employees

Accounting Professionals

Who Do Phishers Impersonate in Phishing Emails?

An executive within a company or organization

Authorities at federal tax organizations worldwide

Requests tax information which may include personally identifiable information (PII) or sensitive W-2 data.

Threaten with legal action, claiming the recipient's company failed to properly file their taxes.

Use reminders or "helpful hints" (like tax breaks), appealing to recipients' uncertainty and desire to take the best route for doing their taxes.

Offer unsolicited tax advice regarding retirement savings.

Offer fake tax refunds in order to hook the user into taking action on the phishing attempt.[1]

Threat actors impersonate tax authorities all over the world

In the first few months of 2017, Cofense identified emails delivering malware from cybercriminals impersonating tax authorities in **Australia, Brazil, India and Italy**.[2]

Types of tax-related phishing emails vary

In March 2016, PhishMe recorded **21 different phishing website templates** being used to create IRS phish.[3]

What Do You Do If You Receive a Tax-related Phishing Email?

Remember

the IRS does not send emails requesting information. Be wary of attempts to gather personal or financial information via emails, text messages or social media channels.

Don't Click on Links in Emails

go directly to your tax authority's website instead of following links when in doubt about the authenticity of an email.

Report Suspicious Emails

to phishing@irs.gov, an IRS security team that's part of the U.S. Treasury Inspector General for Tax Administration

Don't Panic

phishers craft emails that prey on recipients' emotions[5]

Fear **Uncertainty** **Doubt**

Document Everything

Whether you've fallen victim to the scam or spotted the phish in time, it's important to report the incident to your security operations center so that further damage can be prevented.

Never miss another phishing threat again.
Sign up for Cofense's FREE Threat Alert Service!
Visit **cofense.com/threat-alerts**

Sources

1. https://www.ic3.gov/media/2005/051201.aspx
2. "Tax-time Phishing: A Global Problem," Cofense blog post, March 9, 2017.
3. "Tax Time is Phishing Time: Here's How to Help!" Cofense blog post, March 31, 2016.
4. https://www.irs.gov/uac/report-phishing
5. Cofense's "Enterprise Phishing Susceptibility and Resiliency Report 2016"

COFENSE