



Alerts

Practical Tips to Mitigate the Risk of Being Hacked by Fake IRS or Google Voice Scams

November 3, 2021

Law Firm Cyber Alerts

Risk Management Question

What are some of the newest hacking scams that may affect law firms and other businesses?

The Issue

On October 27, 2021, the Federal Trade Commission (FTC) issued warnings to be on alert for two new hacking tricks.

The [Fake Email Alert](#) warned about fake Internal Revenue Service (IRS) emails offering a third Economic Impact Payment (EIP) if the responder clicks a link and provides personal information. The IRS warned this is just another version of the classic government impersonator scam. Clicking on the link enables the scammer to commit identity theft.

The [Google Voice Scam Alert](#) warned about coordinated efforts to steal telephone numbers. The scammers target people who have posted items for sale, are missing pets, or have otherwise posted information online, seeking others to respond and contact them. The scammers then suggest they are concerned whether the person posting the information is a real person and that the posting is not fraudulent. The scammer's approach is to ask for the verification code sent by Google to confirm the poster's identity. The FTC warned that providing the verification code creates an opportunity for the scammer to create Google Voice telephone numbers linked to your original telephone number. The new Google Voice numbers may be used to falsely list items for sale, often using the poster's name in the ads.

Risk Management Solutions

Law firms, their employees, and their clients should consider taking some or all of the following actions, including those recommended by the FTC:

- The government will never call, text, email, or contact you on social media saying you owe money or offer help in getting a third Economic Impact Payment. Your best bet is to visit the IRS's website directly for trustworthy information on EIP payments. (<https://www.irs.gov/coronavirus/third->

Attorneys

Joseph J. De Hope, Jr.

Service Areas

Cyber Security for Law Firms

Law Firm Cyber Alerts

Lawyers for the Profession®



[economic-impact-payment](#)).

- Do not share the Google verification code sent to your phone with anyone. If hackers don't know your code, they are less likely to be able to access your information.
- If you gave someone a Google Voice verification code, follow [these steps from Google to reclaim your number](#).
- Don't share sensitive personal information with anyone without first verifying the recipient.
- Report potential scams and hacks to the FTC at <https://reportfraud.ftc.gov/#/>.

One final tip – if it sounds too good to be true, it probably is too good to be true.