Phishing Red Flags

FROM

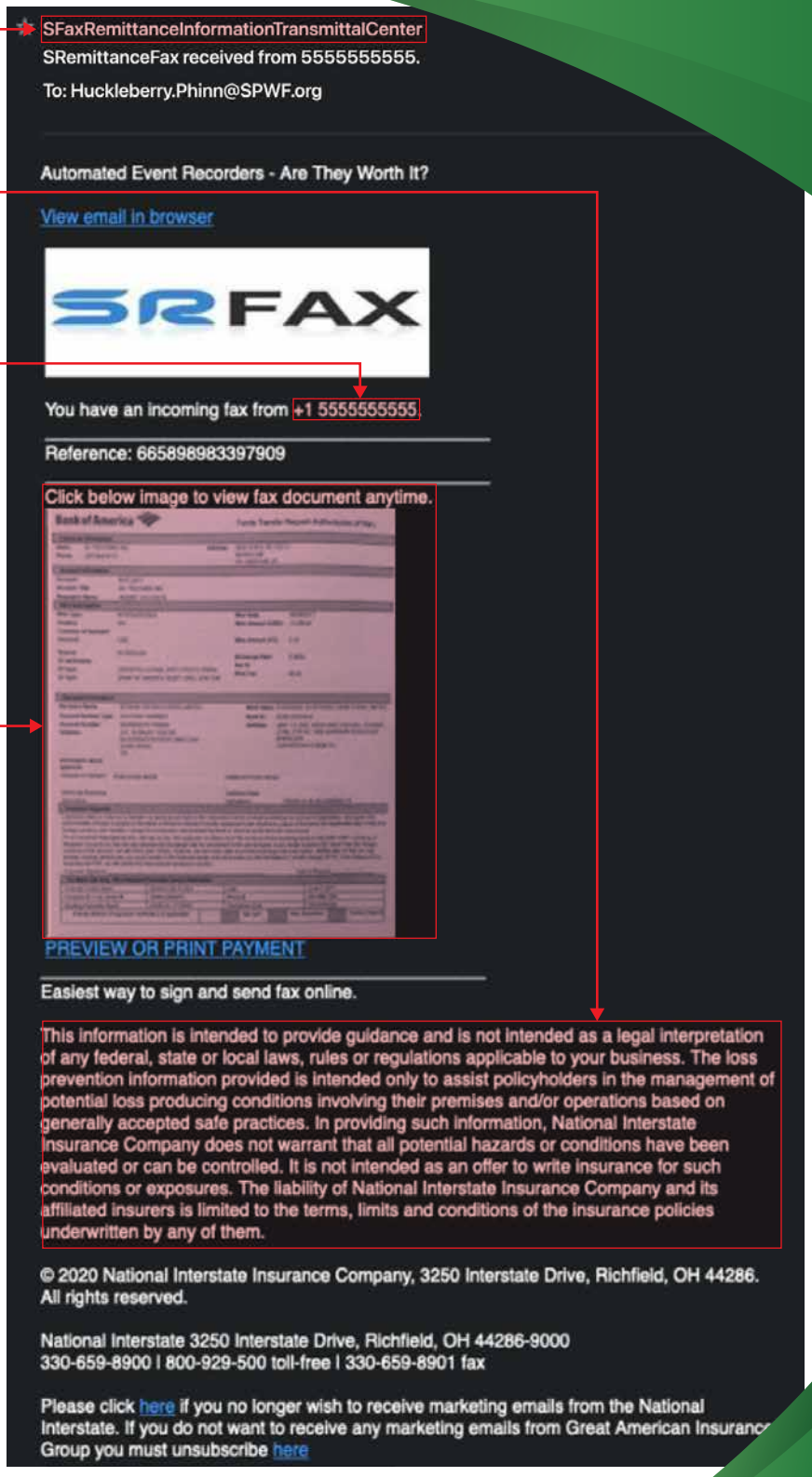
- The email says it's from a fax remittance service, but includes a disclaimer from and links to a law firm in Illinois.

PHONE

- The area code of the fax number is in North Dakota, not Illinois.
- The phone number works but is not a fax number.

CONTENT

- The small, blurry embedded .png image of a document with a Bank of America logo followed by a link to "Click below image to view fax document anytime" enticing the user to click for a higher-resolution image. Highly suspicious.
- If clicked, the links redirect to a OneNote page on a compromised Sharepoint site belonging to yet another unrelated company. Using redirects is another tactic used by malicious actors to obscure the actual link and to avoid detection by email security platforms.
- The OneNote page contains a warning to "Use receiving email to access documents to prevent error". This warning was likely used by the attacker(s) to help ensure that they would compromise Huck's business email credentials as opposed to his personal email credentials.



INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452