CIRSA LOSS ALERT

Published by the CIRSA Risk Control Department | SAFER TOGETHER

Loss Alert – Share File Phishing Attacks

Sharing files via email and the internet can be an efficient way to collaborate and get things done. **But not when it's a cyber phishing attack!**

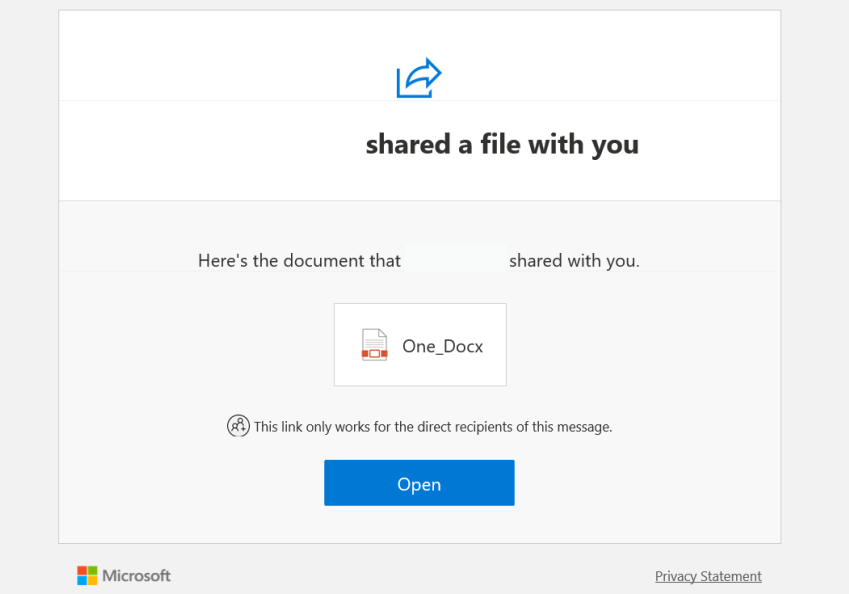
This Loss Alert is to bring to your attention two sophisticated share file phishing attacks that are making the rounds. Normally, our Loss Alerts focus on lessons gleaned from an unfortunate event experienced by a CIRSA member, and we're careful not to reveal the member's identity. This time, though, it was CIRSA that experienced the unfortunate event (and affected some members during the course of the event), so we're "outing" ourselves and sharing some lessons we've learned. Please feel free to forward this email to others in your organization.

The most important thing to keep in mind is to **be cautious about opening share file emails and any links in those emails**, even those that appear to come from known sources.

For employees who regularly collaborate on SharePoint, Google Docs, or similar platforms, receiving share file emails is common. And a spam share file email can be hard to detect. Here's a screen shot of one such email CIRSA recently received (image on next page):

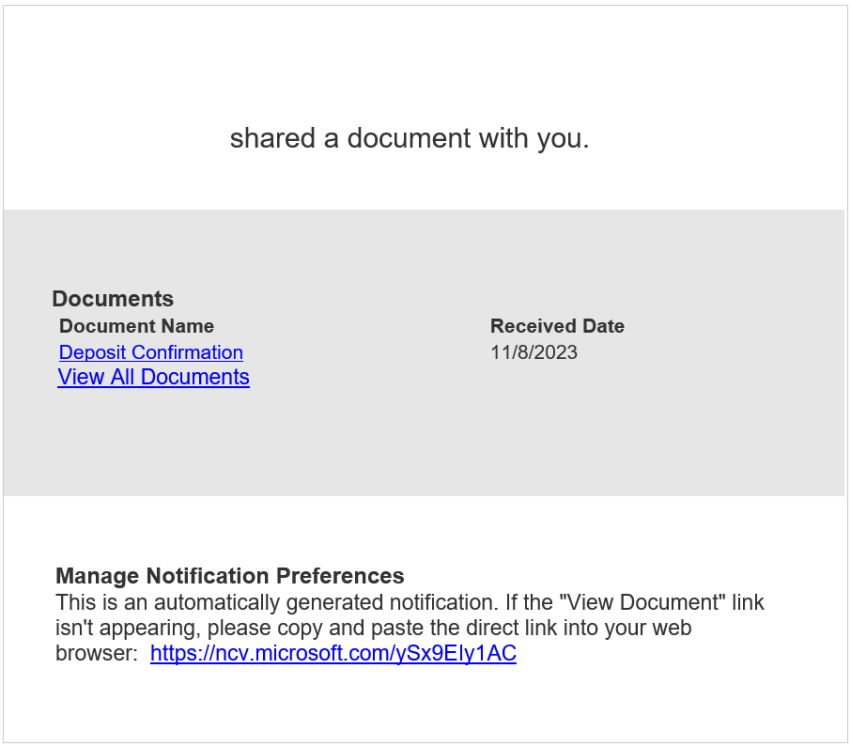
3665 Cherry Creek North Drive • Denver, CO 80209 • 303-757-5475 • 800-228-7136 • CIRSA.org

Share File Phishing Attacks (cont.)



This email looks virtually identical to a legit SharePoint email, and like SharePoint, it allowed the recipient to click on the file and enter their credentials to access the file. But it turns out this email was not legit and clicking/opening its links created a potential pathway for viruses and malware.

Here's a screen shot of another phishing email CIRSA recently received:



Share File Phishing Attacks (cont.)

This one was sent with two embedded links, "Deposit Confirmation" and "View All Documents", that if clicked/opened also created a potential pathway for viruses and malware.

Lessons learned?

- Phishing attacks that are disguised as share file emails can be difficult to spot. Unlike narrative emails, they may not contain as many (if any) of the usual red flags such as typographical errors, bad grammar, unknown names and addresses, or unusual statements that clearly seem "off" or that leave the reader wondering "What the!?"
- Moreover, these share file requests can tug at any reader's inclination to engage; naturally, the reader may be eager to click the linked document to read the latest draft, or click the "deposit confirmation" to see how much money is coming in!
- And when the email purports to be from a known colleague—whose name is front and center, often in large or bolded text—recipients can be all the more trusting.

With phishing attacks becoming ever more sophisticated, what can be done?

First and foremost, you'll want to remind employees to be especially vigilant around opening emails (and especially clicking on links) that are suspicious in any way, even if they appear to come from known sources.

Other important reminders:

- Never click on any links or attachments in suspicious emails.
- Take time to closely review suspicious or unexpected emails. Closely review the sender's email address. Often, a "fake" email address may only be one letter off from a legit one. If it can be done without clicking or opening them, hover over embedded links to review the true location of the URL.
- Erring on the side of caution is the best solution. If you receive a share file email or similar email unexpectedly, without any notification from a trusted source, always assume it is NOT legitimate until you've confirmed with the source or your IT Department that it is safe to open. Even if a share file email appears to come from a person you know, contact that person via some other means such as a text message or phone call to confirm that they sent the message and it is valid.
- Likewise, if you're planning to send a share file invite, an invite to videoconference, etc., first email or text the recipient so they can keep a lookout for a legitimate invite from you.
- If you know or suspect that an email is not legitimate, delete the message and make your IT staff aware of it.
- If in any doubt, always call your IT staff.

Share File Phishing Attacks (cont.)

If your entity recently received from a CIRSA account one of the share file phishing emails depicted above, you should have received an email from CIRSA IT on November 8 confirming the issue has been resolved, and we apologize for any inconvenience the situation caused.

If you are subject to a cyber event, CIRSA's Claim Department is available 24/7/365. If you have a cyber-related event that occurs within or outside normal business hours, please contact us immediately for assistance, by calling (303) 757-5475 or (800) 228-7136. If it's after normal business hours, an answering service will immediately forward your call to a Claims representative. If warranted, the CIRSA representative will set up a consultation with CIRSA's cyber expert attorney at Constangy, Brooks, Smith and Prophete. This consultation will typically include a forensic IT expert.