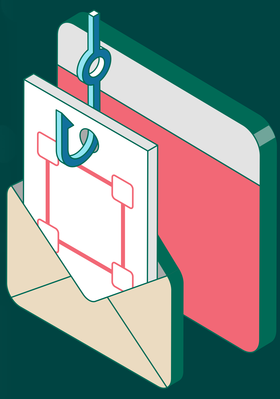
SVG PHISHING

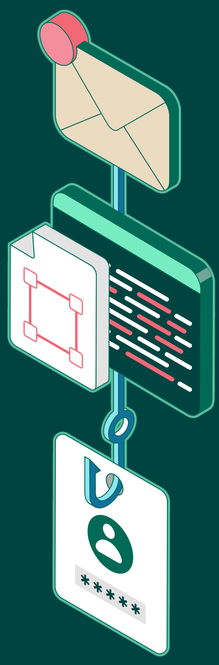


Scalable Vector Graphics (SVGs) are image files made of text, which means they can be resized without losing quality. That makes them ideal for websites and apps that need to look good on screens of all sizes.

Unfortunately, fraudsters take advantage of this format by hiding malicious JavaScript code inside the SVG file. When opened, this code can redirect you to a dangerous website or track your online activity, allowing attackers to impersonate you.

ANATOMY OF A SVG PHISHING ATTACK

- Ping! You get an email:
  - Subject: Invoice Overdue
    Please see the attached invoice. Payment is overdue and must be received before the end of the day tomorrow.
- It's an SVG file, which seems unusual for an invoice, but plausible enough. You click.
- Instead of an image, you're redirected to a page that looks like your company's Microsoft login page. Odd, but plausible. You enter your credentials.
- And just like that, your login information is stolen.
- Cybercriminals are using SVG files to hide malicious JavaScript. These files can silently redirect users to fake login pages or harvest session data for impersonation.
- To lure victims, attackers rely on social engineering techniques:
  - They name files things like "invoice," "voicemail," or "e-signature"
  - They craft emails that look urgent and legitimate
- Users may never know that they were scammed because some SVG phishing scams do not redirect to a malicious site. And those that do may redirect to a site or portal that looks official and even has your organization's logo.
- It only takes one click.



PROTECTING YOURSELF FROM MALICIOUS SVGS

Implement the following best practices:

- Carefully inspect hyperlinked files and attachment extensions, paying close attention to the right- most extension, which indicates the file type.
- Be wary of any SVG attachment or hyperlinked file you receive, even when it appears to come from a trusted contact.
- Never click or open SVG files from unknown senders, or in messages you were not expecting to receive.
- Before clicking or opening a file received via email, always pause and evaluate. If something feels suspicious, report it to our IT team.

SVG files may appear safe, but hidden code can turn them into powerful vectors for sophisticated cyberattacks. Understanding the risks is key to keeping you and our organization safe.