Estate Valuations & Pricing Systems, Inc.
Security Hygiene Guidelines

Overview

Anyone in the world can contact any e-mail address or phone number at EVP Systems, including people with malicious intent. Being alert to the kinds of threats that can arrive via these channels is an important part of the company's security apparatus. Automated software screens every e-mail that is sent to us, but it does not—indeed, cannot—catch everything, nor can it apply common sense to ambiguous situations or evaluate phone calls. EVP Systems is not a high-profile target, but bots, spammers, and phishers usually attack indiscriminately, and pernicious attachments, links, and social attacks have arrived in our inboxes and voicemail in the past, and will again in the future.

Below are some circumstances to watch out for. The presence of these situations is no guarantee that an e-mail or a phone call has harmful content, but even a few together in a single message can be a good indicator that something is wrong.

E-Mail

If you suspect that an e-mail has malicious intent, please forward a copy to `emergency@evpsys.com`, and power down your workstation.

Attachments

- The e-mail is from an address you don't recognize, or is not *to* an address you recognize.

- The e-mail is very generic:

    - It does not address you by name or the name of your company.
    - It does not have a full signature, or does not mention the person or the company sending it.
    - It uses a generic subject, or is a subject line you wrote that is being responded to. ("Urgent Information Needed ASAP!", "Re: Tuesday's Meeting with Rebecca".)
    - Any references to you or your company, or the sender or their company is by information already present in the e-mail: the domain name, the e-mail address, etc. ("Dear john@smithcompany.com…")

- The attachment has a generic filename, or is derived from information already present in the e-mail: the domain name, the e-mail address, etc. (`information.doc`, `smithcompany.zip`)

- The attachment is a ZIP file, with a generic password. (“12345”, for example.)

- The password to the ZIP file is included in the body of the e-mail with the attachment, rather than being sent separately.

- If you open an attachment, it asks you for extra permissions: administrative authority, to enable editing, etc.

Links

- The website that opens when you click on an e-mailed link is flagged by the browser as possibly malicious.

- The website that opens when you click on an e-mailed link asks you to download a file, or a file begins to download automatically.

- The website that opens when you click on an e-mailed link asks you to enter *any* account information, but especially account information for an unrelated system like Microsoft Office 365, Google Workspace, or Dropbox.

- The link shown in the e-mail is subtly misspelled, oddly formatted, from a Chinese or Russian top-level domain, or apparently random. (`goog1e.com`, `paypal.com.systemallowed.anglefire.com`, `dropbox.ru`, `hk23i23987whiu23iu2.com`.)

- The link shown in the e-mail is different from the URL in the browser’s location bar when you click on it.

- Any security certificate on the site was generated by Let’s Encrypt, and created within the past few days.

Each of these warning signs can be “stacked”—meaning piled on top of each other. You can get a legitimate-looking e-mail from a client that links to the real `dropbox.com` website, but the file on Dropbox will be malicious, and ask to be downloaded or for you to click on a link and enter your credentials. Just because the first step seems safe, don’t assume that each step after is.

In addition, if something seems suspicious and you contact the original sender, do it via a different channel than the message arrived. For example, if you received an e-mail from

someone that doesn’t seem right, contact the sender via phone. Their e-mail account may still be held by the attacker, and the response can’t be trusted.

Phone Calls

If you suspect that a phone call has malicious intent, please ask for a call-back number, hang up, and forward the details of the call to `emergency@evpsys.com`.

Social Engineering

Security attacks via the phone can either be initiated by the attacker simply calling the company number, or by prompting you to call a number via a pop-up on your computer (usually accompanied by a scary message about a virus or pornography) or a request via e-mail. The attacker can’t do anything to your system in this scenario without your help, and will use several psychological techniques to get you to provide it: solicitousness, bullying, fear and threats, and so on.

- Any contact with a company should be initiated through their main line, looked up via their website, or a known-good direct contact rather than a number delivered to you via pop-up or an e-mail.

- Never give out client, security or financial information to a caller on a call you did not initiate, or that you have not verified via information not easily available to the general public (such as co-workers, an office address, or a previous balance with EVP Systems).

- Never hesitate to hang up on someone who begins to act unprofessionally, aggressive, or threatens legal consequences for not doing what they ask.

Last Updated: October 13, 2024