March 8, 2019

Guarding Against the Chinese Domain Name Email Scam

Risk Management Question: The Canadian Trade Commission recently issued a warning about a new email scam that involves the sender posing as a Chinese registrar company and attempting to convince the receiver that an existing firm domain or brand name is in danger of being registered by an unrelated third party. In addition to seeking money, the purpose of the scam is to gather more specific information about the firm and its lawyers in order to commence a targeted attack. What can you do to protect yourself and your firm from these email scams?

The Issues: Scammers send emails to companies or law firms purporting to be from Chinese companies that are authorized registrars of CNNIC (China National Network Information Center, the constructor and operator of the information society infrastructure in China) or other official bodies. The emails further assert that a third party has applied for a certain domain name whose keywords are identical to those of the firm. The Canadian Trade Commission reports that the following exploits may be used:

- The Chinese party indicates that they want to, seemingly out of goodwill alone, remind the foreign company or firm of the possible negative consequences of their brand name being registered by others in China. The Chinese party then suggests that the foreign company apply through them for a Chinese domain name—for a fee, of course. Some of these unsolicited e-mails have requested documentation from the foreign company to substantiate their name and trademark, which then could ultimately be used by the Chinese company to their own ends.
- Another version of the scam involves a Chinese company—again claiming to be authorized by an official body—approaching a foreign company warning that its Chinese domain name will expire soon, then asking for renewal fees.
- Yet another scenario alleges an unassociated company having registered a ".cn" domain name that is very similar to a legitimate company's domain name. The associated website is copied directly from the legitimate business, negatively impacting the real company's commercial interests.

One actual scam email reads as follows:

> Dear Sir,
>
> The important affair is about your company name [X Company] registration, please forward it to your company's leader.
>
> Recently we received the registration application from [Chinese Company, Ltd], they want to register the [X Company] brand name and some domain names. As

an authoritative and responsible registrar, we need to confirm if the company is your company's cooperative partner. Also we need to verify whether you have allowed the company to apply these names.

Waiting for your response.

Risk Management Solutions: Should you receive such an email, send it to your firm's IT department for evaluation, and then delete it. And please remember the three key anti-phishing rules:

1. If you receive an email from out of the blue, never click on a link or attachment.
2. If you receive an email from someone you know, but it includes an attachment that you were not expecting to receive, call the sender to confirm it came from the sender and not a hacker.
3. Finally, if you forget rules 1 and 2 and click on something which opens a dialog box asking you to supply additional information—or click on something to enable a later software version or to open a zip file—close it out immediately and call your firm's IT department to have a scan run on your computer.

To these rules, we would add: never provide information about your firm or yourself to someone you don't know, regardless of the form in which the request is made (email, text, or phone call). What may seem like innocuous information can be used by hackers to develop a strategy to target you or your firm.

Remember, let's be careful out there


Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com


Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com


Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com


Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com