Trust is essential and must be earned

My last blog post detailed an ongoing attack on my inbox by a “lead generation company” called Bark. As of today, I’ve continued to receive dozens of emails from both the same sender (“Kate Potter”) or with the same subject line (“new customers looking for your services”). In fact, I got at least six since last night.

But all I have to do is see who the sender is or read the same subject line to hit delete. Bark can continue to send emails until the end of days, and I will never open them. Why? Because I don’t trust that Bark is legitimate. In fact, Bark has earned the opposite reputation, that of a spammer, an illegitimate business that seeks to worm its way into getting you to click or call by sending emails that may have the veneer of legitimacy but are a front for a scheme.

Too many bad actors

Cybersecurity and privacy threats are rampant, and we have to guard constantly against them. There are just too many bad actors seeking to damage businesses and people by installing malware or by phishing to get passwords in order to steal identities.

Clicking on links in emails always opens us up to problems. That is, unless we trust the sender and know they are not acting maliciously.

Reputation matters

In order to keep opening and reading email, we need to trust

the sender. Generally, we trust senders we have a relationship with. We know some senders personally or we've conducted some kind of transaction with them (donation, purchase, etc.) and thus we trust them.

However, if we don't trust the sender, we may not even open the email. And if we do open the email, we are certainly not downloading attachments or clicking on links.

Spammers don't understand trust

Trust is essential in the keeping yourself safe from cyber threats. And that is what Bark and many other spammers don't seem to get. They seems to think that as long as they are hiding behind a *veneer* of legitimacy (looking like legitimate business query or coming from the correct industry), then we will just trust that they are real. But trust is earned. And when you send the same email over and over and over again, you are not earning trust. You are causing suspicion. When you attempt to send the same email from a different sender's names, you are not engendering believabilty, nor are you increasing the chance that the recipient will open the email.

Endnote

I just checked Bark on WHOIS. All information has been "redacted for privacy." In other words, there is no contact information whatsoever. All I can find out from WHOIS is the name of the domain registrar for this "company." And I can use this information to register a complaint.