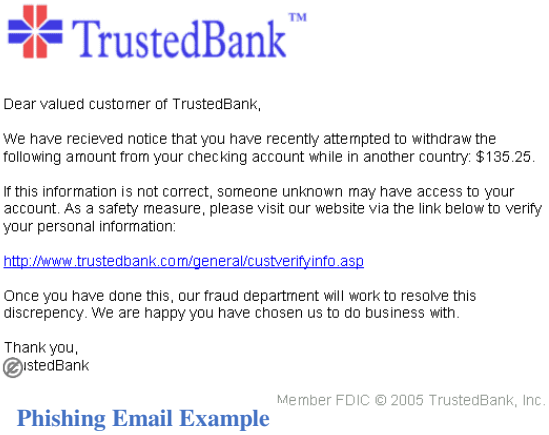
*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

SPF. DMARC. DKIM. Oh My!

We spend a lot of time making sure we have policies in place to protect our institution from reputational risks associated with technology, and even more time is spent on training, auditing, and compliance to manage those risks.

But rarely do we consider what goes on *outside* of the physical or virtual perimeter of our networks.

Consider this: what would you say if I told you that there is a 79.7% likelihood that a third party is either actively sending email as if it came from your domain without your knowledge, or has in the past?


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing Email Example

Don't get all bristly; hear me out. According to a recent report by 250ok, almost 80% of published domains do not have any type of domain level email authentication configured. Domain level email protection can be implemented easily with very little time and effort, and it's likely you can get your support contracts and agreements to do the work for you.

There are three ways to combat fraudulent email sent on your behalf to either external *or* internal recipients at the domain registration level.

Before we get into that, let's talk about Spoofing. Spoofing is the act of impersonating a device or person to steal data or bypass access controls. As you can guess, email spoofing is the act of sending email on behalf of some domain that you don't own or control. Plain and simple, unless it's expressly allowed by the DNS record owner, email spoofing is identity fraud.

So how do we combat this fraudulent activity?

Let's start with Sender Policy Framework, or the open standard for SPF text records. Most domain registrars – think GoDaddy, Network Solutions, Domain.com, etc. – support SPF, which allows administrators to define the IP addresses or hostnames allowed to send mail on behalf of a particular domain. A well-crafted SPF text record should contain the IP addresses and hostnames of any externally facing mail service that is allowed to send email from or on the behalf your domain… that's right, you can allow legitimate spoofing. There are rules, standards, and limitations for the use of SPF records. Contact your DNS registrar for information on how to create an SPF text record for your email domain. If you are using Office 365 or hosted email, reach out to the provider.

Next is Domain Keys Identified Mail or DKIM. This standard is similar to the way websites and web-based data transactions are protected using SSL certificate (HTTPS). Like SPF, the DKIM standard requires a text record to be created by your DNS registrar that contains a public encryption key. The legitimate sending email server is configured to generate and insert a unique DKIM signature in the sent email's header information. The recipient email server then uses the unique signature to compare against the public DKIM records and if the signatures match then the email is considered authentic and is sent on to the intended recipient.

Lastly, and more complex than SPF and DKIM is DMARC, or Domain-based Message Authentication. DMARC is considered an enhancement to SPF and DKIM. It allows the email owner to dictate how an email is handled should it fail the authorization tests provided by SPF and DKIM. Properly configured SPF and DKIM records must exist before DMARC can be used, and if not properly configured DMARC can break mail flow.

In conclusion, to process SPF, DKIM and DMARC records you must have properly configured DNS records, as well as a properly configured email server or service, or an email security appliance at the perimeter.

At a minimum, implement SPF or DKIM. The effort is worth it. It might just save you and your customers a lot of headaches from fraudulent email-based attacks and will prevent the attacks from looking like they originated from your servers.

Authored by: Mike Smith, AWS CCP