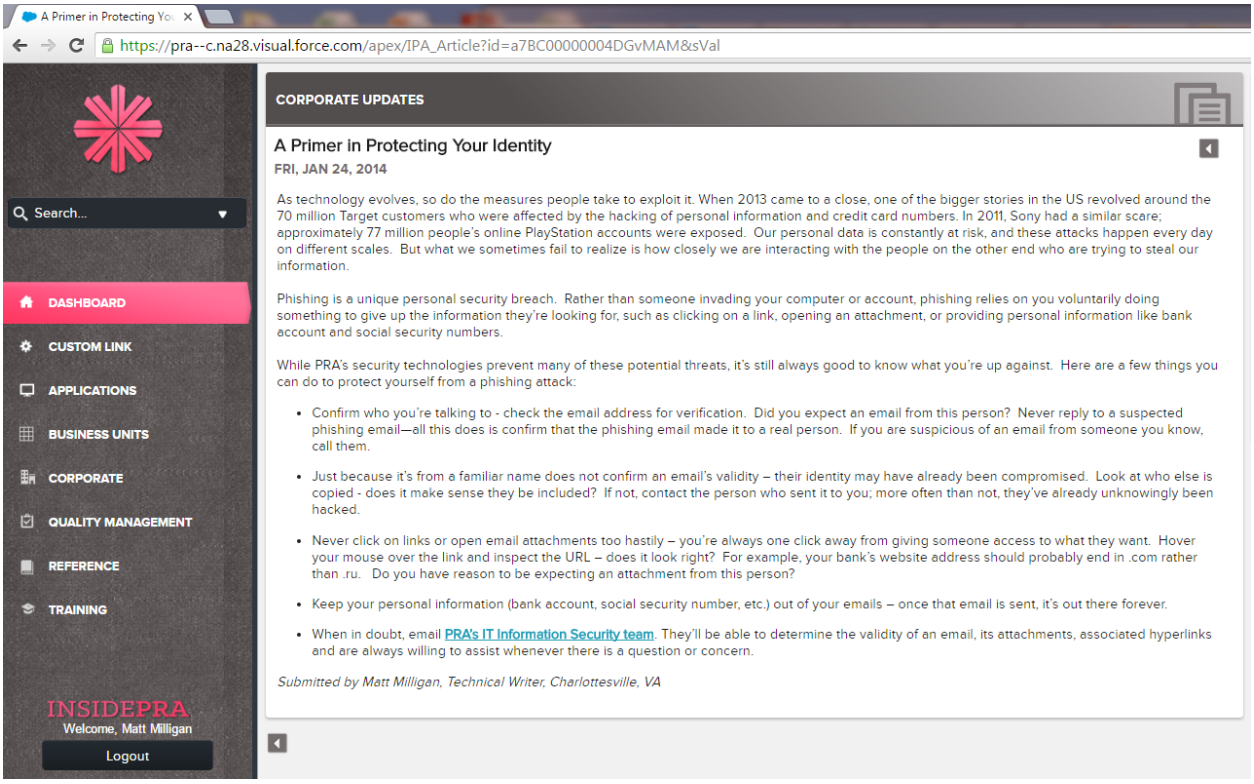
Internal Security Article
January 24, 2014

Synopsis: at the close of 2013, one thing had become abundantly clear: email phishing attempts had not only become more frequent, but increasingly clever. We had seen an uptick in Help Desk requests related to falsified emails, specifically ones disguised as internal users. I was approached with the idea in mind that we start generating an awareness internally about keeping our users protected without seeming like we were 'scolding' them. The result was a series of articles posted on the company intranet aimed at keeping people informed about the perils of online information security in <u>and</u> outside of work.

Visual context:



A Primer in Protecting Your Identity

As technology evolves, so do the measures people take to exploit it. When 2013 came to a close, one of the bigger stories in the US revolved around the 70 million Target customers who were affected by the hacking of personal information and credit card numbers. In 2011, Sony had a similar scare; approximately 77 million people's online PlayStation accounts were exposed. Our personal data is constantly at risk, and these attacks happen every day on different scales. But what we sometimes fail to realize is how closely we are interacting with the people on the other end who are trying to steal our information.

Phishing is a unique personal security breach. Rather than someone invading your computer or account, phishing relies on you *voluntarily* doing something to give up the information they're looking for, such as clicking on a link, opening an attachment, or providing personal information like bank account and social security numbers.

While PRA's security technologies prevent many of these potential threats, it's still always good to know what you're up against. Here are a few things you can do to protect yourself from a phishing attack, whether you're at work or at home:

- Confirm who you're talking to – check the email address for verification. Did you expect an email from this person? Never reply to a suspected phishing email – all this will do is confirm that their phishing email made it to a real person (you!). If you are suspicious of an email from someone you know, call them to verify.

- Just because it's from a familiar name does not validate its authenticity, as their identity may been compromised. Look at who else is copied – does it make sense they be included? If not, contact the person who sent it to you; more often than not, they've unknowingly been hacked.

- Never click on links or open email attachments too hastily – you're always one click away from giving someone access to what they want. Hover your mouse over the link and inspect the URL – does it match up with what they described? For example, your bank's website address will almost certainly end in .com rather than, say, .ru. Do you have reason to be expecting an attachment from this person?

- Receive an email saying you've had an account hacked? Do not rely on <u>any</u> information contained in it, as it may be disguised to look legitimate. Do a quick internet search for your institutions customer support number, and call them directly. They'll be able to corroborate any suspicious activity on your account.

- Keep your personal information (bank account, social security number, etc.) out of your emails – once that email is sent, it's out there forever.

- When in doubt about something you've received, email [redacted]. They'll be able to determine the validity of an email, its attachments, and associated hyperlinks. Better safe than sorry!