The ZeroFont Email Phishing Scam and How What You Can't See Can Hurt You

June 21, 2018 - Users of Microsoft's Office 365 are susceptible to phishing scams using a technique dubbed ZeroFont; a means by which scam artists can get their email though Microsoft's email filters. It's an old trick that allows you to send an email message that looks different to mail filters than it does to the recipient. Here is what you need to know.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
 (function() {
   var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
   po.src = 'https://apis.google.com/js/plusone.js';
   var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
 })();
```

Microsoft uses natural language filters to scan all incoming mail messages. These filters look for key words and phrases to identify scams and phishing attacks. For instance, a mail message that contains the words "Microsoft" and "password" that doesnâ€™t' come from a legitimate domain might be flagged. Using the ZeroFont technique, scammers can fool the system.

ZeroFont allows the sender of the email message to insert characters into the message with a font size of zero. Those characters won't be visible to the message recipient, but they are visible to Microsoft's filters. For instance take the following string of characters and imaging that the characters in red have a font size of zero: itsMic1986roNAMEsptu:of32t. Microsoft's natural language filters would see the entire text string. But only the word "Microsoft" would be visible to the recipient of the message. And that's a problem.

The goal of the people sending the message is to make sure that it winds up in your inbox rather than in your spam folder. They know that if the message if flagged as spam, there is almost no chance that you will become their victim. But if they get the message past the filters, there is a chance that you will.

On the other hand, Microsoft's goal is to protect you. To do that, they flag words and phrases that are common in phishing attacks using natural language filters. But if those filters see a character string like the one shown above, they think they are looking at large text block with randomly generated characters, so they don't work.

Right now, there really isn't anything that Office 365 users can do to protect themselves unless they subscribe to an outside screening service such as Boxbe. But this requires a separate investment and isn't necessarily desirable for anyone in sales because it makes it more difficult for your customers and prospects to contact you.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS