File Transfer Phishing Attack Rears Its Ugly Head Again

August 17, 2018 - About three years ago there was a phishing attack making the rounds claiming that "someone has sent you a file." Email messages in the attack appeared to come from WeTransfer; a popular European file transfer platform. The attack was fairly easy to spot because it the person who supposedly sent the files was never named. Well, the attack is back and now it does name names.

Once again, the attack starts with a phishing email, but from someone you probably know. Once someone clicks on the links in the message, they are taken to a fake website and asked to enter some information. By the time the attack is over, your email account and your address book have been compromised. In the end, your friends, colleagues and family will be very quickly targeted in just the same way. And the mail messages they receive will appear to come from you.

You may think that this sounds like a silly attack. But there is real value in compromised email addresses; especially when those addresses can be linked with a friends listâ€¦ meaning the people in your address book. This information can then be sold on the dark web to be used for other scams. This is especially problematic when employers' email systems become compromised.

Anyone who gets caught up in this scam needs to change all of their email passwords and should seriously consider changing any passwords for other sights that might be stored on their computers. They also need to notify anyone in their address book that their email was compromised and tell them not to open any messages from them without first making a phone call.
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.