

@foregoystemsinc



Fifth Third Bank. PayPal. eBay. Citibank. Dr. Mombassa from Nigeria. And many, many others. What do they have in common? Scams.

The internet has made it easy for the bad guys to scam the good guys. Have you ever received an email from the Fifth Third Bank saying that your account may have been compromised, and that you need to “click here” and log in immediately to confirm your settings, otherwise your account may be closed by Security? Or perhaps you’ve received a similar message from PayPal or eBay or another bank, like Citibank.

You aren’t being legitimately notified. You are being scammed. The scammers, many of them overseas in Eastern Europe or the Far East, are simply searching for your log-in information so that they can steal your identity, run up your credit cards, or generally wreak havoc in your life.

By using “legit” graphics, the scammers try to make you believe that the emails are actually coming from Fifth Third Bank, etc., when in reality the log-in doesn’t take you where you think you are going. If you were to examine the HTML code, you’d see that instead of going to eBay or PayPal, you were going to some overseas address, and your information was going to end up in a database, and into the hands of scammers, just waiting to fleece you for whatever they can.

So how do you recognize legit emails? Well, first of all, never, ever log-in to a website that requires a username and password from an email. Just don’t do it. If you have an eBay account and you get an email from eBay telling you to log-in for some reason, and they provide you with a little form in the email to do so...you aren’t going to be logging in to eBay! It’s the policy of legit companies NOT to

@foregoystemsinc

give you those types of log-in screens. Instead, if they are legit, they will tell you to go to their website and securely log in. Now, be careful here too...some scammers will say the same thing in their plea to you. "Don't be fooled by scammers!" they will ironically state, "Don't ever log-in from an email. Go to the main eBay site, by clicking **HERE**, and safely log-in." Except that by clicking that "HERE" button to supposedly go to the real eBay home page, you will start your journey down the road to the dark side. Scammers will even host pages on secure servers to outsmart you. Scammers aren't dumb by any means. They will do almost ANYTHING to get you to believe them.

And then there are the letters from the Nigerian [substitute many African countries here] who has \$26,400,000 that he wants to transfer to your bank account, where you can keep 25% as a helper's fee, so his "wife and thre graet [sic] children" can escape the terrible civil war going on in their homeland. Note the use of misspellings to supposedly make it sound more authentic. Again, these are scams to get your personal information.

The best advice? If something seems too good to be true, avoid it like the plague. If an email says "Log in!" just don't. If the message IS from eBay, trust me, they'll be very happy if you simply go to their site and log in. No legit company is going to ask you to log-in via email, nor should they provide you with a button to get to their site.