What to do if you receive a phishing email whether it results in a financial loss or not?

Description

We all know that the title industry is under attack and phishing emails are on the rise becoming more sophisticated. It is every agentâ??s worst nightmare to think they may fall victim to a phishing email and suffer a financial loss. It is important to be prepared with the information beforehand on what steps you should follow in the event you are a victim of a phishing email whether you suffer a financial loss or not.

VLTA Examiner

The FBI reporting agency for phishing emails or other Internet related scams is the Internet Crime Complaint Center, www.ic3.gov. IC3 was formed in 2000 as a central place that all Internet crimes are to be reported whether they result in a financial loss or not. IC3 takes all data, analyzes it, and disseminates it for investigative and intelligence purposes to law enforcement agencies. IC3 is an important piece for identifying trends and areas that phishing emails are coming from. Understand that you will not hear back from IC3 even if you are submitting information regarding a financial loss. IC3 is for data collection purposes only and will pass important information along to the FBI for further investigation.

If you do suffer financial loss due to a phishing email scam you need to do all of the following quickly:

1. Contact the Bank
2. Contact the FBI
3. File report with www.ic3.gov

The quicker you act the better the chances you have at recouping funds.

If you do NOT suffer a financial loss due to a phishing email scam it is important that you still report all information to www.ic3.gov. By doing this you are playing vital role in assisting IC3 with categorizing trends and identifying where the phishing scams are originating from.

The real estate industry is the fastest growing industry with phishing email scams resulting in financial loss seeing an increase of 1100% since 2015. The average loss for other industry scams is $9,000, the average loss for a real estate scam is $120,000. It is important to stay vigilant and train employees to do so as well. We are all in this together, share your experiences with each other and/or your

underwriters to get the word out.

Special thanks to Melissa Ellis of SME for contributing this information.

Category

1. Cybersecurity

Date Created
2018/06/05
Author
vltaexaminer

VLTA Examiner