In February 2022, users of NFT marketplace OpenSea were the victim of a [phishing attack](https://halborn.com/what-is-phishing-attack-techniques-and-examples/).  The attacker managed to steal tokens from exploited users that were later sold for $1.7 million in ETH.

**INSIDE THE ATTACK**

The OpenSea attack began as a phishing email [asking OpenSea users to migrate their NFTs](https://twitter.com/ishwinder/status/1495238247290703873) to a new OpenSea contract.  The goal of this attack was to trick OpenSea users into signing an order for a transfer of 0 ETH on OpenSea.  This order included the attacker’s address and the calldata for the order, which was legitimately signed by the phished user.

The attacker [takes this order and adds the addresses and calldata](https://twitter.com/Nesotual/status/1495223117450551300) for all tokens for which the user has approvals on OpenSea.  The attacker then calls their own malicious contract with this order.  From there, the legitimate order is sent to OpenSea.

OpenSea performs validation of the signatures on the contract before processing any orders.  Since the user was tricked into signing the order and the attacker also signed it, both the maker and taker contracts are valid.  The OpenSea contract then calls the proxy contracts that hold the approvals for each of these tokens.

These proxy contracts use delegatecall to call the attacker’s contract, which is the target of the transfer.  With delegatecall, the attacker’s contract can perform transactions on behalf of these proxy contracts.

This delegatecall executes a function in the attacker’s contract that loops through a list of the addresses and tokens for which the user has created approvals.  With the context of the proxy contract and these preexisting approvals, the attacker can steal all of these tokens from the phished user’s account.

**LESSONS LEARNED FROM THE ATTACK**

The OpenSea hack was made possible by a phishing attack in which users signed orders without validating them.  Since these orders were designed to send tokens to a malicious contract, the attacker was able to take advantage of pre-existing approvals on the NFT marketplace to steal all tokens for which these approvals existed.

This hack underscores the importance of validating transactions and the danger of approvals.  Without a valid, signed transaction and approvals for tokens, this attack could not have happened.