# ACCOUNT TAKEOVER AND LATERAL PHISHING | AN INSIDE LOOK


## Step 1: External Recon

Scammers research target companies and organizations using information found easily on the internet through web searches and professional and social networking sites.

## Step 2: Infiltration

Using this information, they send phishing emails to their targets in the hope they'll click on a link that secretly gives them access to their account and network.

## Step 3: Internal Recon and Pivoting

Scammers can now set their sights on any intel of value that can be leveraged to suit their needs.

## Step 4: Engagement

Armed with the accounts and information they need, the cybercriminals craft and send phishing emails designed to distribute malware, facilitate wire fraud or perpetrate other scams.

## Step 5: Monetization

A successful attack results in a transfer of money from the victim to the criminal who often continues scamming undetected under legitimate-looking cover.

## Lateral Phishing

Lateral phishing, an offshoot of account takeover, occurs when compromised accounts are used to scam others within the accountholder's network.

The victims are typically business partners or vendor companies who rarely suspect their legitimate email contact is a scammer in disguise.

## So, what can you do to help prevent these attacks?

It starts with a robust information security culture that emphasizes training on how to identify suspicious phishing emails, especially internal ones that can be highly sophisticated.

These can include odd email send times or points of origin. Unusual phrasing, language or references can also be a giveaway.

A skilled information security firm can also provide perimeter, inbox and human based security in a multi-layer approach that can fortify your business against these threats.

Barracuda®
Your journey, secured.