



# Rollout Guidelines

## Account Takeover and Lateral Phishing

Conducting a phishing simulation is easier when you have the right tools. The following tips and content will help you plan and execute your campaign your way, so you can train and inform effectively.

- Choose any email in the Barracuda PhishLine content center that you feel best targets your employees to see if they could be compromised. Link it to the ‘You’ve Been Phished’ landing page.
- Link the landing page to the **Account Takeover** module so that employees who click the link can learn more about the topic (optional).
- Use the Account Takeover **Spotlight** and **Infographic** to supplement training by distributing as desired.
- As always, contact Barracuda PhishLine support with questions or if you would like assistance.

### Email

Your choice from the Barracuda PhishLine content center

### Spotlight

**Click Thinking Spotlight**  
Account Takeover and Lateral Phishing

Account takeover and lateral phishing are so effective because they provide cybercriminals with a perfect cover for their scams. Legitimate business email accounts that have been compromised for their own...

- Business email is a high-value target for cybercriminals because it provides access to sensitive information and can be used to impersonate the sender.
- Lateral phishing is a type of phishing attack that targets employees who have access to sensitive information.
- Account takeover is a type of phishing attack that targets employees who have access to sensitive information.
- Account takeover and lateral phishing are so effective because they provide cybercriminals with a perfect cover for their scams.

### Landing Page Phished Tiles

**YOU'VE BEEN PHISHED!**

LET'S LEARN FROM THIS EXPERIENCE

- Phony sender:** 40%
- A sense of urgency:**
- Phony links:**
- Poor Spelling and Grammar:**
- Recipient issues:**
- Dirg consequences:**
- Agree to Etootion:**
- Research, report incidents:**

### Training Module A103A—20

**ACCOUNT TAKEOVER & LATERAL PHISHING**

### Infographic

**ACCOUNT TAKEOVER AND LATERAL PHISHING | AN INSIDE LOOK**

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

**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.

**Internal Recon and Pivoting**  
Scammers can now see their sights on any level of value that can be leveraged to suit their needs.

**Engagement**  
After gaining the account and information they need, the cybercriminals craft and send phishing emails designed to distribute malware, facilitate wire fraud or persuade other users.

**Monetization**  
A successful attack results in a number 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 account holder's network.

**So, what can you do to help prevent these attacks?**  
It starts with a robust information security culture that empowers training on how to identify suspicious phishing emails, especially internal ones that can be highly sophisticated.

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.