

# Rollout Guidelines

## PCI—DSS

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 the email, **Payment Card Compromise Check**, and landing page, **You've Been Phished**, from the Content Center and build your campaign around them.
- Link the landing page to the **Payment Card Compromise Check**, module so that employees who click the link can more about the topic (optional).
- Use the PCI-DSS **Spotlight** and **Infographic** to supplement training by distributing in common areas.
- Keep materials out for a set period of time, but don't leave them out too long or employees may lose interest.
- As always, contact your Barracuda PhishLine support or your consultant if you have questions or would like assistance.

### Email—Payment Card Compromise Check

**Payment Card Check**

Input your account number, indicate card type and refer to the color guide to see if your information may be compromised or on the dark web.

enter account number

☐ credit ☐ debit ☐ credit ☐ debit ☐ credit ☐ debit ☐ credit ☐ debit

> **Warning.** Your card information is on the dark web.  
 > **Caution.** No dark web presence but card may be compromised.  
 > **Nothing Reported.** Your card can't be traced to the dark web.  
 > **Very Secure.** Your card cannot be traced and is protected by the issuer.

If the card information you provided shows up red or orange, please notify your issuing company for details and possible preventive action.

Payment Card Check was developed by SecureShare, a non-profit organization dedicated to helping individuals build and maintain stronger online networks. Patent pending #28-15613238. © 2018 SecureShare. All rights reserved.

### Landing Page—You've Been Phished



### Infographic



### Spotlight



### Training Module A103A—13

