



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 #28-51643238. © 2019 SecureShare. All rights reserved.

Landing Page—You've Been Phished

YOU'VE BEEN PHISHED!

The error you just obtained was a test to see how you'd respond. Had this been a real phishing attempt, your actions could have led to a compromised account.

LET'S LEARN FROM THIS EXPERIENCE
Recognizing errors have immediate benefits. You can protect yourself and the company by learning to recognize them.

Phony sender Look closely at the sender name. A phony sender may look like a legitimate business.	Recipient issues Large numbers of compromised recipients or links that are not being received.
A sense of urgency Requests for information often accompany phishing emails. It's a ploy to make you act.	Dire consequences Threats of negative consequences unless you click on a link or provide sensitive information.
Phony links Hover your mouse over links and the URL will display. For example, it could be something like: http://www.paycom-software.com	Appeals to Emotion Emotional language or graphics that cause you to panic or feel fear.
Poor Spelling and Grammar Phishing emails often contain spelling and grammar errors.	Remember, YOU'RE IN CONTROL. If you're unsure if you've been phished, report it. Don't click on links or provide sensitive information. WHAT YOU SHOULD DO: Report the phishing attempt to your IT department.

Infographic

PCI—DSS
Payment Card Industry Data Security Standards

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Continuously Monitor/Security Controls
- Maintain a Security Awareness Program
- Enact Strong Access Control
- Establish and Maintain a Robust Information Security Program

Barracuda

Spotlight

Click Thinking Spotlight
PCI—DSS

Payment cards are the backbone of most commerce. Understanding Payment Card Industry Data Security Standards can protect both those who use them and the companies that process them.

- It's important to understand the Payment Card Industry Data Security Standards (PCI DSS) framework to better understand and identify risks from falling prey to the wrong links.
- A secure network includes a variety of protection controls designed to protect the sensitive data exchanged when sending the information to an online merchant website or to a system connected to other nearby computers.
- An information security program also includes secure email software, if used on company computers, at your request or if required by your state, state or federal law or industry regulations to protect sensitive data and any communications about sensitive data that are sent from mobile.
- Most data breaches involve some sort of user engineering. PCI DSS requires a security awareness program that includes user fire and account training to help employees understand how to handle their data.
- Regular security vulnerability scans, a need to know basis and regular updates to web browsers and operating systems. Regular updates to software also should also be installed.
- Establish a program that collects and reports information about phishing attempts, similar to other security programs.
- Make sure guidelines are clearly communicated, and that training is available to help staff understand the correct security.
- Educate the organization on PCI DSS and its responsibility to understand the guidelines and its importance to the business and how to handle phishing and other security threats that can be valuable to your company.

PCI-DSS

Training Module A103A—13

PCI—DSS

PCI DATA SECURITY STANDARDS
WHAT YOU NEED TO KNOW