

ANGLER PHISHING PROTECTION

SAFEGUARD YOUR SOCIAL MEDIA CUSTOMER SUPPORT INTERACTIONS

Customers like the convenience of receiving customer service through social media because they know their complaints and questions will get a prompt reply. More than 80% of their inbound social customer service requests now happen on Twitter.¹

As a result, cyber criminals have turned this into a ripe opportunity to steal credentials using angler phishing attacks. This is a dangerous form of support fraud that targets your customers when they reach out to your Twitter account for help.

Angler phishing is a significant risk to your company and customers. We've already seen angler phishing jump 200% year over year from Q3 2016 to Q3 2017.² As part of managing and securing your company's digital engagement, it's important to protect your customers from angler phishing attacks.

HOW DOES ANGLER PHISHING WORK?

Cyber criminals create highly convincing customer service accounts and then wait for your customers to reach out to your brand with a help request. Automated listening tools make it easy for criminals to monitor your social accounts to find a potential victim. They often strike on evenings or weekends when your customer service teams are less likely to monitor the account for requests.

When the fraudster sees a customer contact your brand account, they intercept the communication and send a reply from the lookalike support account.

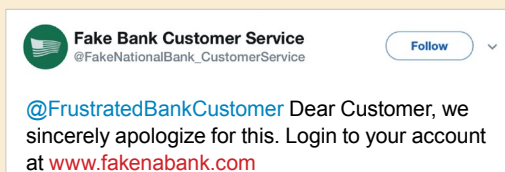
The criminal usually assures your customer they'll resolve the problem quickly and directs them to a lookalike site where your customer is invited to log in. By doing so, your customer inadvertently hands account credentials and sensitive data to the criminal.



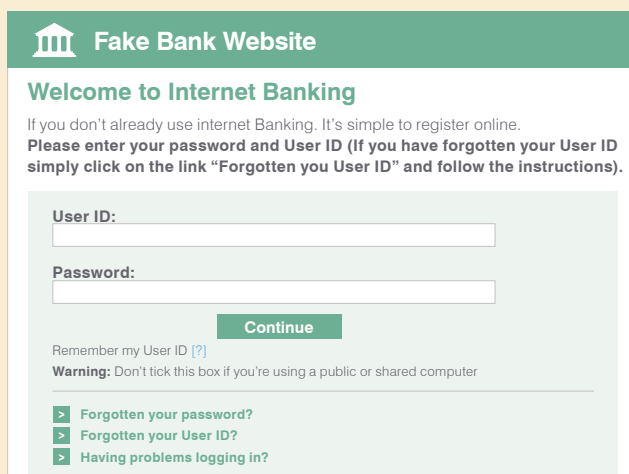
ANGLER PHISHING USE CASE



1 Frustrated customer tweets at @bank



2 Fraudulent account monitors tweets @bank and responds with fraudulent domain link



3 Customer follows link to fake domain, logs in, and their credentials are stolen

¹ Twitter. "Making customer service even better on Twitter." February 2016.

² Proofpoint. "2017 Q3 Quarterly Threat Report." October 2017.

PROTECT AGAINST ANGLER PHISHING WITH PROOFPOINT

Angler phishing is a risk for any business that provides customer service on social media. Criminals can create and take down lookalike support accounts in minutes. When it comes to safeguarding your customers, time is of the essence.

Proofpoint Angler Phishing Protection is the only patent-pending solution that continually uncovers fake customer service accounts and infringing domains that put your brand and customers at risk.



Protect Against Social Customer Account Fraud

Angler Phishing Protection monitors your social customer care interactions around the clock and detects angler phishing attempts on your customers. We notify you immediately when someone contacts your customers from a fake customer care account, so you can initiate your response plan.



Discover Fraudulent Domains

Attackers set up lookalike domains and web pages that are designed to trick your customers into giving up their credentials or other sensitive information. Angler Phishing Protection continually analyzes and detects newly registered domains that present a potential threat. We notify you immediately when we detect suspicious domains that need enforcement.

IMPLEMENT AN ANGLER PHISHING RESPONSE PLAN

Proofpoint Angler Phishing Protection gives you the visibility you need to implement a response plan for handling active angler phishing attacks. Your plan should include the following:

- 1. Ownership:** Assign owners who are responsible for 24x7 coverage of the response plan.
- 2. Customer Communication:** Fast and clear customer communication is an essential part of your plan. Consider a few communication systems that will help you quickly reach your customers.
- 3. Triage:** Identify the appropriate steps that will protect your customer and your system while you address the threat. Consider placing a temporary lock on your customer's account while you contact the customer and manage triage.
- 4. Takedown:** Contact Twitter to take down the fraudulent customer support account and monitor the status until the account is closed.

PUBLISH YOUR SUPPORT GUIDELINES

Putting security at the center of your social governance processes will help you get a handle on angler phishing. Define your standard security practices and include the appropriate customer guidance on your Twitter account, including:



Social Media Support Hours

List the hours your team monitors your social media support account to provide live responses. Consider asking customers to submit inquiries only during posted support hours. This can reduce the window of time for bad actors to carry out angler phishing attacks.



Communicate Your Security Practices

Let your customers know your security protocols for account login and other standard requests. For example, "We never ask customers to log in from a link within the Twitter session. We'll always direct you back to our official home page if your support inquiry requires an account login."

Angler Phishing Protection helps you remove the risks of angler phishing and preserve the quality of your customer service interactions.

LEARN MORE

To learn more about Angler Phishing Protection visit: proofpoint.com/angler-phishing-protection.

KEY BENEFITS

Angler Phishing Protection helps you:

- Gain real-time angler phishing threat monitoring
- Protect your customers from credential and identity theft
- Discover fraudulent domains and social customer care accounts
- Preserve the quality of your customer engagements
- Implement an angler phishing response plan
- Improve your security practices and customer guidelines

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.