frogworks

Managing Your Technology So Your Business Doesn't Croak.

2023

Issue 12 Volume 13

Ribb"IT" Review

INSIDE THIS ISSUE:

Beware of the Phishing Campaign Targeting Dropbox

A new phishing campaign is making the rounds in an attempt for hackers to obtain sensitive information from vulnerable users. This campaign, first uncovered by tech researchers at Checkpoint, targets the popular cloud storage platform Dropbox. Learn more about the cybersecurity threat and how you can stay safe.

How the Dropbox Phishing Campaign Works

This clever campaign has several parts to it. Let's review how hackers execute their plans step-by-step.

Dangers of Phishing

Hackers create ways to trick users into giving out their personal information, such as with deceptive emails or links to fake websites. They use messaging that claims a user needs to act urgently and provide sensitive data, such as credit card numbers or banking information. Once the hackers have this data, they can do with it as they please and wreak havoc on unsuspecting people.

The dangers of phishing extend to business owners, their employees, and beyond. Victims must deal with the following issues:

- Financial loss or identity theft
- Violation of safety
- Lack of trust online

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944

Beware of the Phishing Campaign Targeting Dropbox (cont)

Hackers Host a Document on Dropbox

The plan begins with unknown bad actors creating a Dropbox account. They host a benign document that looks like a file from OneDrive and send phishing emails to users. Dropbox users will see a button that says "view document." If they click, it leads them to malicious links. Hackers can implement the next phase after users end up on this site.

Distribution Phase

A key part of this Dropbox phishing campaign is getting users to a malicious site to harvest their credentials. Once someone ends up on this page, their information is given to cybercriminals who can use it against them. If you fall for the first part of the plan and have hackers stealing your credentials, it can be challenging to feel secure online again.

Why This Attack Is Hard to Recognize

Checkpoint reports that thousands of users have fallen victim to this attack. It's particularly challenging to avoid since hackers use Dropbox's system to share files and notify other users via email. Since the email comes from a reputable source, hackers can bypass any email scam filters or other protective measures you set up. This ultimately makes you more likely to open malicious links.

The best way to keep your information safe from bad actors is to always be on guard. Refrain from assuming every email you receive is secure; report it immediately if something seems a little off. Experts recommend that business owners take the time to educate their employees on safe practices and report any suspicious email to an IT professional.

Protect Your Business from Threats

Every phishing campaign is different, but the threat remains the same. Keep your business safe from hackers by always staying alert and tracking widespread online campaigns.

Booking.com Multistep Phishing Campaign

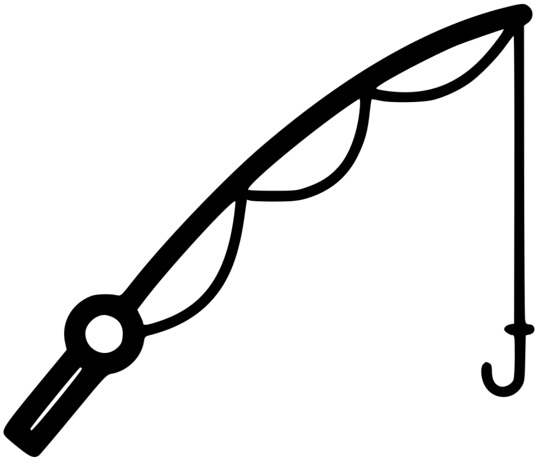
One of the most common ways hackers manipulate online users is through malicious phishing campaigns. The popular travel reservation site Booking.com is the latest company at the center of a targeted cyberattack. Learn more about the dangerous ways hackers infiltrated the site and its impact on countless customers.

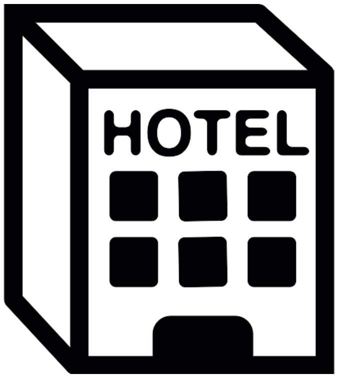
How Phishing Attacks Work

Cybercriminals aim to steal personal information from vulnerable users through phishing attacks. This common type of cyberattack usually involves impersonating a service provider, such as a bank or company. Users often receive messages demanding urgent action and payment information. Credit card thieves behind the attack then take any information provided to steal a user's identity and make unauthorized purchases.

Understanding the Booking.com Phishing Campaign

The hackers behind this large-scale campaign were able to execute their plan in a few steps. Discover exactly how this attack targets users below.





Hackers Gain Unauthorized Access To Hotel Systems

The elaborate campaign begins with cybercriminals infiltrating some hotel systems within Booking.com. Once they can access the hotel's account, they can obtain the booking information of guests who reserve their stay through Booking.com. This first step gives hackers the names, emails, and partial payment information of customers.

Booking.com Multistep Phishing Campaign

Users Receive Phishing Messages

The next step in this phishing campaign is to send messages to the compromised users, urging them to verify their payment information. The phony phishing email tells customers that their hotel reservation will no longer be valid if they don't confirm their payment information within the next 24 hours.

The email also includes a link to a domain that mimics Booking.com. Once users end up on the page, they'll find all their personal details already within contact forms and are asked to add their credit card information to complete the request.

Hackers Steal Credit Card Information

Any users who go to the fake website and enter their credit card numbers unknowingly give this sensitive information to cybercriminals. Once the hackers have the data, they can use it as they please. Victims often find out about their compromised financial information through unauthorized purchases on a credit card statement.

How To Avoid Phishing Attacks

Hackers hope that users will fall for a phishing attack by believing the information presented to them. However, experts encourage you to follow this advice to avoid a cyberattack:

- Thoroughly examine URLs to see if they're legitimate.
- Use caution if you receive urgent requests.
- Contact service providers directly to confirm if they requested information.
- Look for any unauthorized transactions and monitor your accounts.

These steps can help you safeguard against bad actors looking to steal your personal information.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER