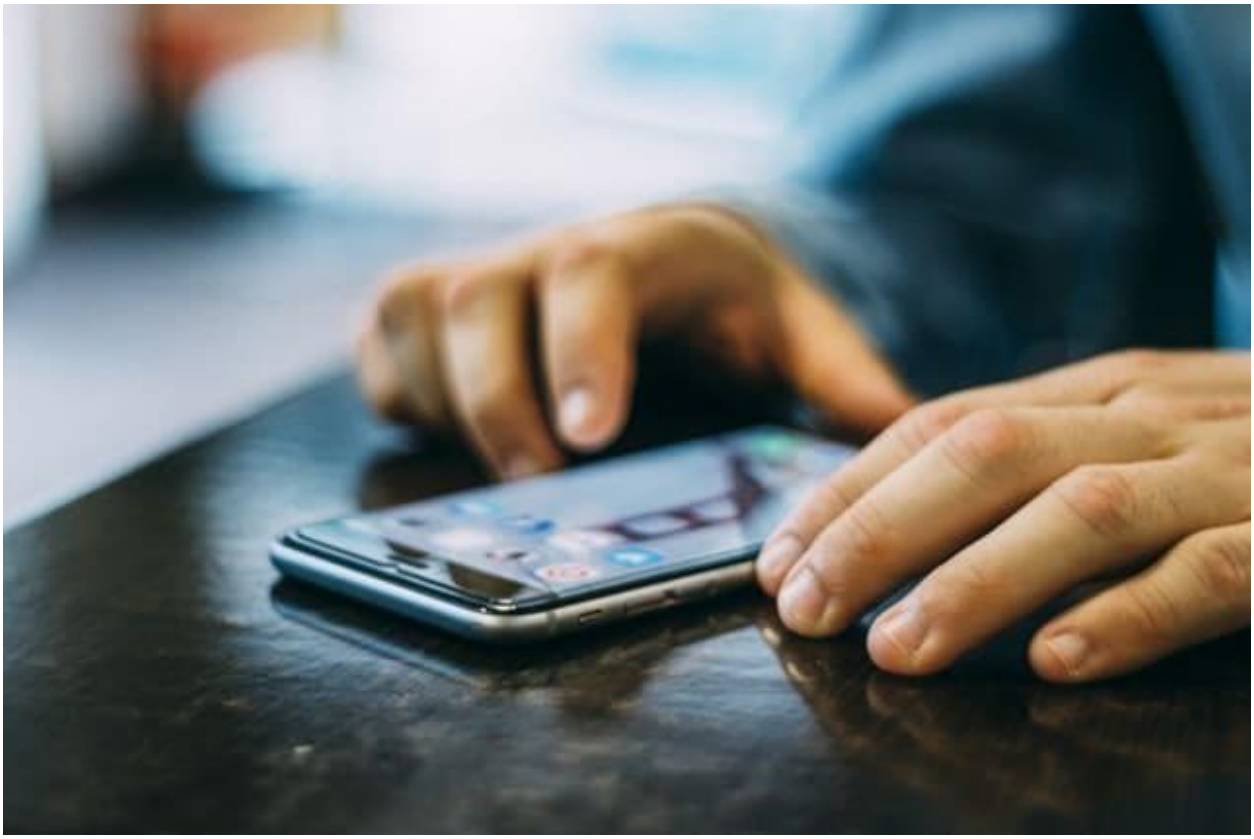
Infographic: Developing Threats in Mobile Phishing

By PinchasNovember 6, 2017blog



In the past decade, we have seen malware, man-in-the-middle attacks, and data leaks as the important and widespread threats for organizations leveraging on mobile devices. However, another, and possibly the most overlooked but equally dangerous mobile attack on the rise today: the mobile phishing.

While mobile phishing isn't entirely new, it has gotten the attention of data security experts and CISOs around the world. To better understand how this security threat works, we've discussed in this infographic what mobile phishing is, and the different techniques being used to defend against this attack.

What is Mobile Phishing?

Basically, mobile phishing is just phishing targeted at mobile device users of an enterprise. According to CSO, phishing is a "well-known and well-understood attack predicated on social engineering…"

For instance, a malicious individual may want to create a mechanism that will help them retrieve important data such as personal or financial records. To do this, they

might use an email, text message, social posts, or other method to lure a victim to a fake website where the victim unintentionally enters personal information for the attacker.

Here are few disturbing statistics from PhishLabs about phishing:

- Phishing volume grew by an average of more than 33% across the five most-targeted industries.
- Attacks targeting government tax authorities have grown more than 300% since 2014.
- Ransomware attacks, the predominant type of malware being distributed via phishing, are now focusing on organizations that are more likely to pay ransoms, such as healthcare, government, critical infrastructure, education, and small businesses.
- The share of attacks against targets in the United States continues to grow, accounting for more than 81% of all phishing attacks.
-

Developing Threats in Mobile Phishing

1. SMS Phishing

Perhaps the oldest style of mobile phishing is through SMS messages. In this method, the attacker sends a text message with a single link to a fake account login page. For example, the message may trick the user to click on the link to "reinstate and upgrade" their profile on a website by which the user is a member of.

While this technique does employ some degree of social engineering, the information it attempts to collect is fairly basic such as the user name and password of the user on the actual website that the attacker replicates. However, even if the victims do not complete the 'phishing' process, attackers gain incremental bits of information necessary to facilitate identity theft – allowing them to gain access to important information of the user, such as their bank account.

2. Phishing through Malicious Apps

In this method, the attacker creates a nefarious application masquerading as the legitimate application. While not isolated to Android devices – especially if the iPhone device is jailbroken – this is generally an issue for Android because users may choose to download apps from other sources due to cost savings and extra features.

However, these apps, while appearing legit, are dangerous. For untrained eyes, malicious apps can look exactly like the original app, but with added features. For example, record fields like user name, password, account number, social security number, etc. The attacker distributes this malicious app on various websites and app stores so that gullible victims can easily find and install them.

3. Phishing Through Modifying Content Within an Application

In this method, the attacker tampers or modify the content within an application. Many mobile apps in the market today display web-based content via an internal browser. Through that web-based content, exploits like man-in-the-middle attack can be employed to modify the content being shown. Once the attacker can influence the web-based content, they can trick the user into giving their user name and password, for instance. This information gets recorded even though the app itself wasn't compromised and never intended to show the malicious web content.

4. URL Padding

URL Padding is one of the most recent mobile phishing technique used by attacker. According to PhishLabs, URL Padding works by "including real, legitimate domains within a larger URL, and padding it with hyphens to obscure the real destination." For example, this phishing URL:

hxxp://m.facebook.com————————-validate—-
step1.rickytaylk[dot]com/sign_in.html

While the URL starts with m.facebook.com (the genuine web address of Facebook mobile) the *actual* domain, in this case, is rickytaylk.com. While the URL itself is not convincing, it does point to an almost exact replica of Facebook's legitimate mobile login page.

Now, if the link is accessed through a desktop computer, the user can easily figure out by hovering the link that the link is fake. However, since this attack is targeted at mobile users, detection is much more difficult. This is because the mobile address bar in mobile phones is much smaller and does not allow for the entire address to be visible. Hence, the only thing visible will be the part which shows the Facebook address.

How to Combat Mobile Phishing?

- Educate and train employees around best practices in mobile security. This should include the principles of responsible communication practices, such as never clicking on links, unsolicited emails or those shared through mobile apps.
- Always use the official apps for sensitive sites.
- Be careful with URLs. On mobile devices with a larger screen, switching to landscape mode may reveal the full URL. If you're using a smaller phone, tap on any suspicious URL, so you can quickly scroll through it in its entirety.
- Avoid sharing business credentials or personal information with anyone via unsecured mobile communication platform.
- Have a security solution in place that can monitor and capture any traffic directed at phishing sites. As a fundamental technique in the hacker's toolkit, phishing domains form the cornerstone of most attacks.

TeleMessage

DEVELOPING THREATS MOBILE PHISHING

In the past decade, we have seen malware, man-in-the-middle attacks, and data leaks as the important and widespread threats for organizations leveraging on mobile devices

However, another, and possibly the most overlooked but equally dangerous mobile attack on the rise today: the mobile phishing.

While mobile phishing isn't entirely new, it has gotten the attention of data security experts and CISOs around the world.

To better understand how this security threat works, we've discussed in this infographic what mobile phishing is, and the different techniques being used to defend against this attack.

WHAT IS MOBILE PHISHING?

Basically, mobile phishing is just phishing targeted at mobile device users of an enterprise. According to CSO, phishing is a "well-known and well-understood attack predicated on social engineering..."

For instance, a malicious individual may want to create a mechanism that will help them retrieve important data such as personal or financial records.

To do this, they might use an email, text message, social posts, or other method to lure a victim to a fake website where the victim unintentionally enters personal information for the attacker.

Here are few disturbing statistics from PhishLabs about phishing:

- Phishing volume grew by an average of more than **33%** across the five most-targeted industries.
- Attacks targeting government tax authorities **have grown more than 300% since 2014.**
- Ransomware attacks, the predominant type of malware being distributed via phishing, are now focusing on organizations that are more likely to pay ransoms, such as healthcare, government, critical infrastructure, education, and small businesses.
- The share of attacks against targets in the United States continues to grow, accounting **for more than 81% of all phishing attacks.**

DEVELOPING THREATS IN MOBILE PHISHING

1. SMS Phishing

Perhaps the oldest style of mobile phishing is through SMS messages. In this method, the attacker sends a text message with a single link to a fake account login page.

For example, the message may trick the user to click on the link to "reinstate and upgrade" their profile on a website which the user is a member of.

While this technique does employ some degree of social engineering, the information it attempts to collect is fairly basic such as the user name and password of the user on the actual website that the attacker replicates.

However, even if the victims do not complete the 'phishing' process, attackers gain incremental bits of information necessary to facilitate identity theft – allowing them to gain access to important information of the user, such as their bank account.

2. Phishing through Malicious Apps

In this method, the attacker creates a nefarious application masquerading as the legitimate application.

While not isolated to Android devices - especially if the iPhone device is jailbroken - this is generally an issue for Android because users may choose to download apps from other sources due to cost savings and extra features.

However, these apps, while appearing legit, are dangerous. For untrained eyes, malicious apps can look exactly like the original app, but with added features. For example, record fields like user name, password, account number, social security number, etc. which the legitimate version of the app does not have may appear on fake apps.

The attacker distributes this malicious app on various websites and app stores so that gullible victims can easily find and install them.

3. Phishing Through Modifying Content Within an Application

In this method, the attacker tampers or modifies the content within an application. Many mobile apps in the market today display web-based content via an internal browser.

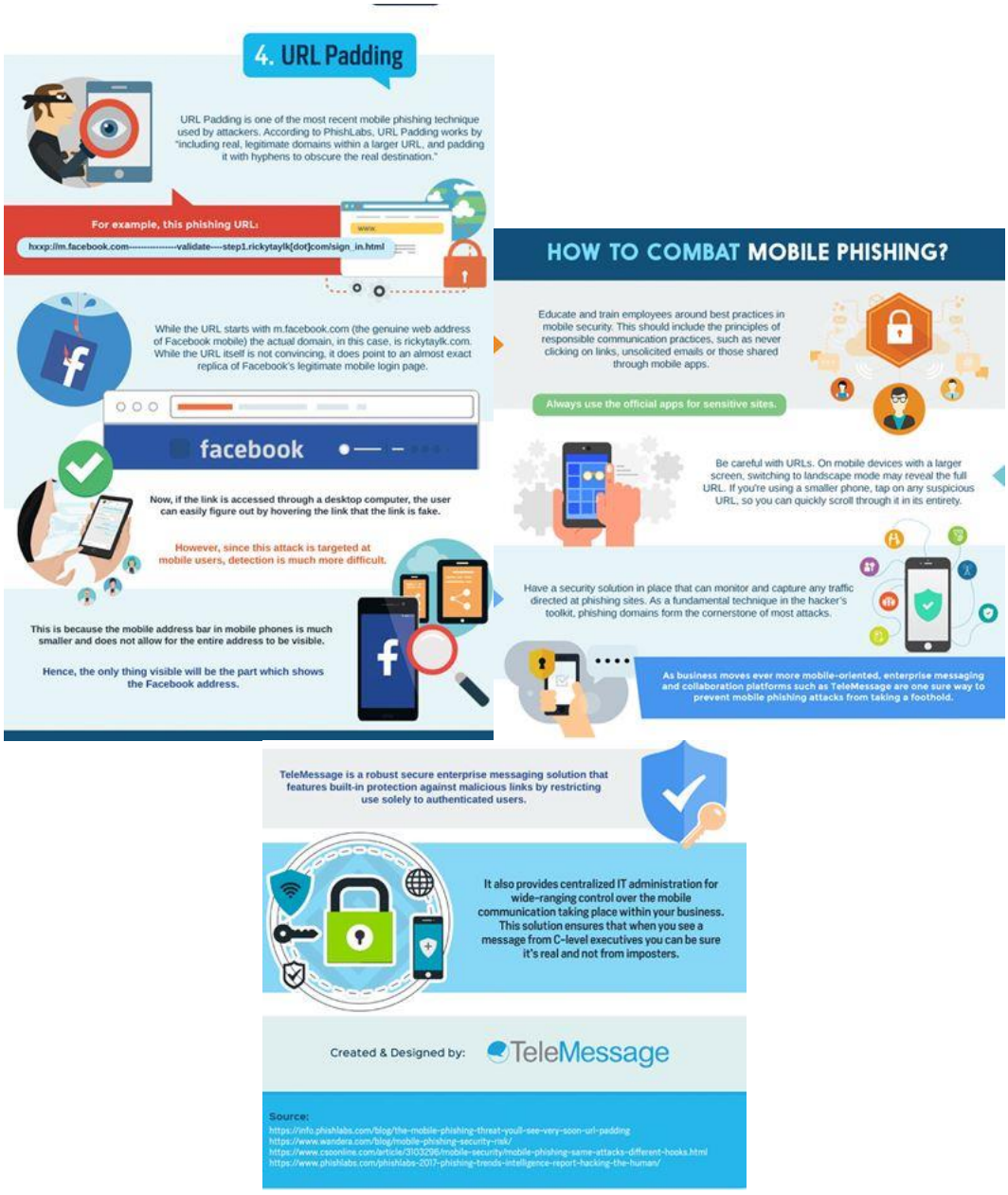
Through that web-based content, exploits like man-in-the-middle attack can be employed to modify the content being shown.

Once the attacker can influence the web-based content, they can trick the user into giving their user name and password, for instance.

This information gets recorded even though the app itself wasn't compromised and never intended to show the malicious web content.

Username

Login



As business moves ever more mobile-oriented, enterprise messaging and collaboration platforms such as TeleMessage are one sure way to prevent mobile phishing attacks from taking a foothold.

TeleMessage is a robust [secure enterprise messaging solution]() that features built-in protection against malicious links by restricting use solely to authenticated users. It also provides centralizranging control over the mobile communication taking place

within your business. This solution ensures that when you see a message from C-level executives you can be sure it's real and not from imposters.
To learn more about our secure enterprise messaging platform, visit our website today at www.telemessage.com