Corrata
IMMUNE SYSTEM FOR MOBILE

Briefing Note

The Rising Threat of Social Media Phishing Attacks

Introduction

Phishing, attempting to fraudulently acquire sensitive personal information from an unsuspecting user, is a well-known cyber threat in today's digital world. For years, cyber criminals have successfully stolen the personal details of internet users through malicious websites and links sent via email. But as cyber-security has developed, users and technologies have gotten smarter. Most employees are now well-educated about the dangers of following links sent from unknown sources online and anti-phishing solutions are widely available to block spam or phishing content from reaching email inboxes. However, as the world becomes ultra-mobile, these protections are no longer adequate. Mobile has created a powerful new channel for hackers to exploit and carry out malicious phishing attacks, particularly over social media and messaging services.

The information-sharing nature of social media sites has made them ideal channels for malicious bodies to impersonate or compromise the accounts of reputable organizations or users in order to build trust and con other users into disclosing sensitive information. Preying on this weakness and abusing the trust of users has proven to be a much more effective form of phishing than email-based equivalents. In 2017 Facebook disclosed that up to 270 million accounts were illegitimate while Twitter identified over 70 million fake and suspicious accounts in 2018. Many anti-phishing solutions however, still fail to protect from social media-based attacks and many users remain unaware of the dangers that may be lurking in their newsfeed.

Social Media Platforms:

WhatsApp

WhatsApp has become one of the most commonly used channels for social media phishing attacks. While one of the most popular smartphone apps in the world with over 1.5 billion monthly users, it has also become one of the riskiest and most commonly blacklisted apps by enterprises due to the high volume of phishing messages currently in circulation. Generally, these messages will warn or offer advice to the user about upcoming changes due to be introduced to the app and will urge them to share the message to their contacts. This social engineering tactic immediately gains the trust of the user as they receive the warning from a friend, family-member, or known contact, and therefore are not given any reason to doubt the content of the message.

For example the 'Martinelli' video and 'WhatsApp Gold' scams, two of the biggest WhatsApp scams in recent years that have been circulating on the app since 2016, encourage users to pass on the chain-mail type messages to their contacts to warn them of upcoming threats or changes. WhatsApp users in countries including the US, Norway, India, and Pakistan have also reported receiving messages offering a free pair of Adidas shoes to celebrate the 93rd anniversary of the brand, that direct them to a legitimate-looking website where instead of claiming the new shoes, inputting their credit card information signs them up for a $49.99 monthly subscription service.

LinkedIn

LinkedIn is a relatively new platform for phishing that has become extremely popular in recent years, likely taking advantage of the assumption that all users are professionals looking to build their network of contacts. Once connected on the site, hackers with false accounts can gain access to users' email addresses and can then spam or lure the user into downloading malware onto their device. Due to the professional nature of LinkedIn, people are likely to accept requests from anyone, unlike Facebook or email, and with access to personal details on the user's profile, hackers can easily personalize communications and build trust. Another common hoax involves creating a fake account for someone in a highly regarded position of a well-known company in order to build credibility and trust among professionals in that industry. Numerous LinkedIn users have also reported receiving emails claiming to be from the website itself with warnings that their account will be deactivated unless they follow a (malicious) link and accept an updated "Services Agreement and Privacy" policy.

Facebook

At the core of every phishing scam is the attempt to look legitimate and gain the trust of the victim. One of the easiest ways of doing this is to pose as a friend or well-known brand, parties in which we implicitly place faith due to their familiarity, and Facebook is an ideal platform for this. Users have been found to be more comfortable clicking on links, downloading apps, or divulging personal information having been prompted or asked by someone they assume to be a friend. A common Facebook scam involves the hacker sending a friend request to a user and once accepted, then posting a message to the victim's wall with a link and an intriguing message such as "Jump on this unbelievable offer before it's too late!". By trusting that this is a legitimate friend and following the link, the victim is brought to a seemingly legitimate Facebook login screen where they are asked to re-enter their username and password. What the user does not know however is that this page does not belong to Facebook and has in fact copied their login credentials and given the hacker access to their account. Once a hacker has control over the user's account, they can then repeat the process and target other users by posing as a trustworthy friend.

Facebook Messenger is also becoming a popular channel to send links to this imitation login page. Last year, it was discovered that a weakness in Facebook's "View As" feature could have allowed hackers to take control of over 50 million user accounts. The most troubling aspect of this scam is the fact that once a hacker gains control of one online account, accessing a user's other accounts becomes easier due to the common use of single passwords and usernames for

multiple accounts.

Twitter

All social networks, especially Twitter, provide the perfect channel for sharing machine-generated content due to their access to extensive personal data, bot-friendly API, colloquial language, and use of shortened URLs. This is often used by brands and companies to distribute content and engage with customers, however it also creates the ideal platform for machine-generated phishing attacks. Commonly, Twitter phishing campaigns take the form of tweets from accounts posing as well known brands or as Twitter itself. In 2016, a study found that 19% of social media accounts appearing to represent top brands were fake, with many of these posing as customer support accounts on Twitter. Taking advantage of the fact that many customers now prefer to seek support from brands over social media rather than through traditional channels like phone, users have been advised to be aware of the blue checkmark badges distributed only to verified accounts and to watch out for slight misspellings or variations in user handles. For example @AmazonHelp is Amazon's legitimate support account compared to @Amazon_Help, a fake account used to steal personal information from users.

Earlier this year an ad was found to be circulating Twitter that claimed users could have their account verified by clicking on the link supplied. Similar to the Facebook attacks, users would then be brought to a page that looked extremely similar to Twitter's official login page where they would be asked to enter their login details, contact information, and follower count. Of course, like on Facebook, this page was fraudulent and was designed simply to steal the user's information.

Instagram

Now with over 1 billion active monthly users, Instagram has quickly become one of the most popular social networks in the world. Inevitably however, this has made the platform a prime target for spear-phishing attacks. Like Facebook and Twitter, hackers gain users' trust by masquerading as friends or followers and then posting links to malicious or phishing websites on their account or via direct messages. Extremely convincing fake login pages are then used to collect account credentials.

What is most worrying about these attacks is that victims often have no idea that they have been targeted, as the fake page simply redirects them back to their Instagram page as if nothing happened. This means that hackers could potentially access or take control of the account for some time without the user ever realizing that their data has been compromised, putting other accounts or sensitive data at risk.

Snapchat

Snapchat is a relatively new platform for phishing attacks, however with 188 million daily active users and its mainly young teenage market, malicious attacks are increasingly common. In 2017, it emerged that a phishing attack resulted in the usernames and passwords of over 50,000 users becoming publicly visible online. The attack relied on a link, sent to users through a

compromised account they believed to be a friend, that when clicked on opened a website designed to mimic the official Snapchat login page. Similarly to the attacks via Facebook, Twitter, and Instagram however, the page was in fact used to collect usernames and passwords, which were then made publicly available on phishing website 'klk.viral.org'.

Response

Social networks are taking some action to detect and protect against suspicious activity. For example, Facebook have vowed to take steps to improve security and privacy features by requiring Two-Factor Authentication for logging in, while Snapchat have introduced the use of machine learning techniques to look for suspicious links sent within the app and block access to suspicious URLs.

Users have also been advised by both security experts and the social media sites themselves to take caution when following links or accepting content from other users online, to navigate to social media accounts of companies or brands from their official websites and to check that accounts have been officially verified, to be wary of clicking on external links regardless of their source, to double check with friends and followers if suspicious of their online behavior and generally, to be cautious of any special offers that may seem too good to be true.

Corrata Security and Control:

As humans however, it is inevitable that we will make mistakes and may be fooled by these cyber frauds. To ensure protection for our sensitive data, especially as organizations with employees using mobile devices for personal as well as business, external security is essential. Corrata's Security and Control solution provides unparalleled protection against phishing attacks, on all platforms. Our SafePathML machine learning technology creates an enterprise grade firewall with complete visibility over device and network traffic. This allows Corrata to detect and block access to any malicious or fraudulent site, allowing employees to continue using services like WhatsApp, LinkedIn, Facebook, Twitter, Instagram and Snapchat, all with the peace of mind that their sensitive data is protected.

Want to find out more about phishing attacks and how to ensure your mobile devices are protected?
Contact Corrata today