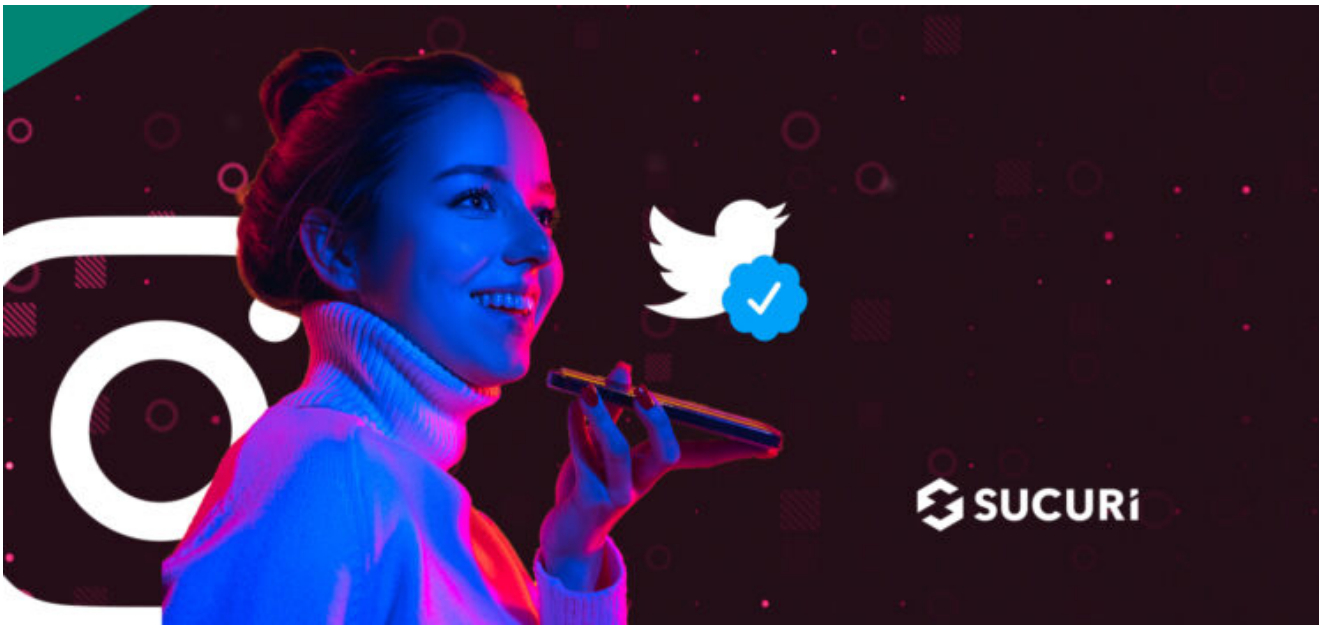
Sucuri Blog

blog.sucuri.net/2022/08/fake-instagram-verification-twitter-badge-phishing.html

Luke Leal August 9, 2022



Social media platforms like Instagram and Twitter offer verification badges as a credibility indicator to help show authenticity and integrity to visitors. To obtain a badge, profiles must meet a list of various requirements and undergo verification process.

For example, the one found on our Sucuri Twitter profile:

Let's examine how these coveted verification badges are being used as a phishing lure for social engineering campaigns targeting some of the most popular social networks across the net.

The Quest for Instagram Verification

The reality is that actually getting an account verified *can* be difficult. Instagram's guidelines explicitly state that users must be a public figure, celebrity or brand and meet certain account and eligibility requirements.

Strong requirements have led to a sort of exclusivity around Instagram's verification badges — in fact, it's become something of a social media status symbol (that money alone can't buy).

Instagram's explosion in popularity and exclusivity of verification badges has made verification highly desirable for many users — a sentiment which also exists on other social media platforms like Twitter.

> I want to be verified on Instagram. I crave that blue check next to my name. Why? Basically because none of my friends are verified, so the verification will prove I'm better than them; which I always suspected.

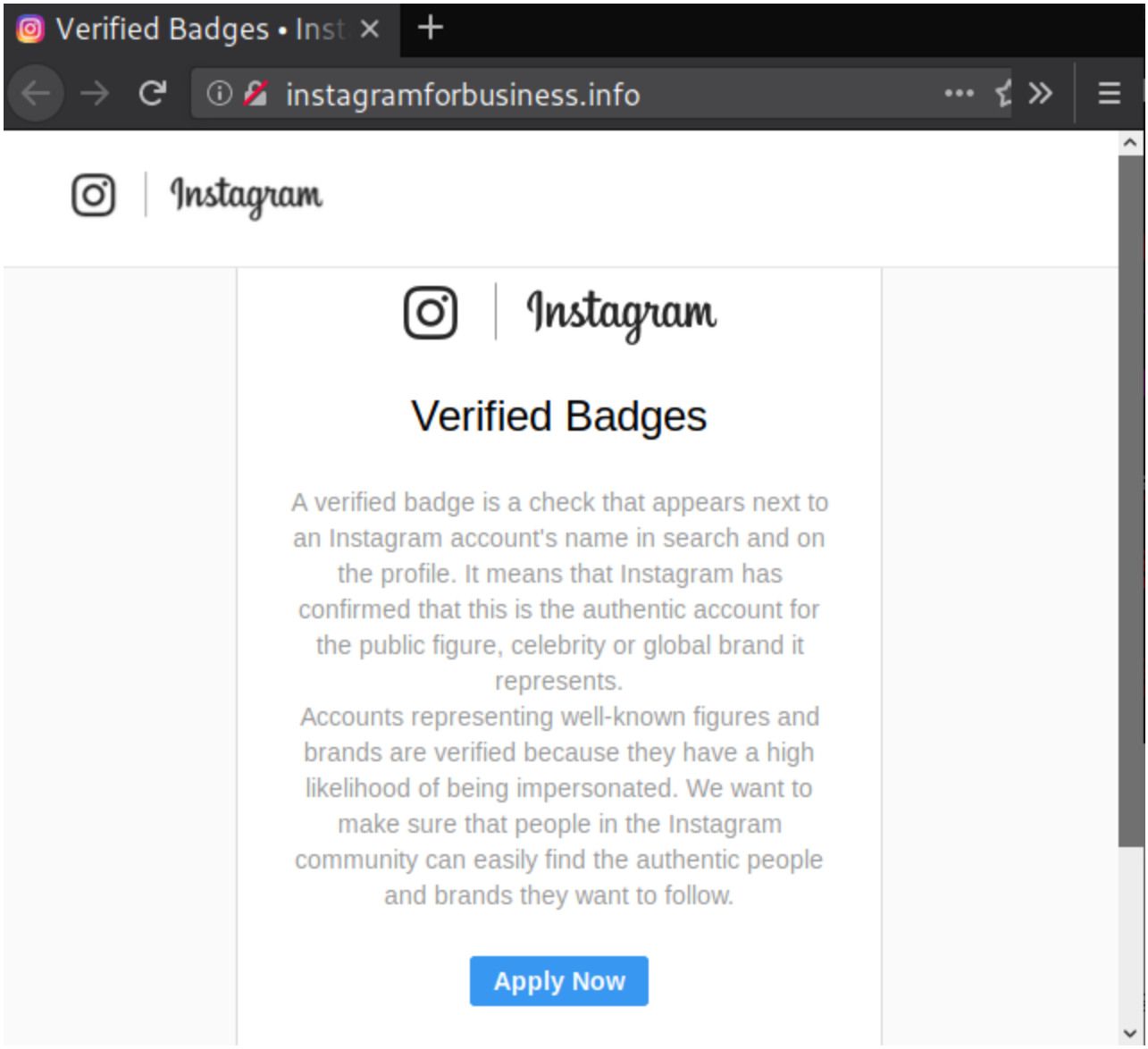
– A joke by the writer showcasing the desire many users have for being verified

While the majority of users may want the verification symbol for bragging rights, the symbol can also help monetize an IG page — and this is driving some users to pursue *any* way possible to obtain the coveted verification for their profiles.

Phishing for Instagram's Blue Badge Verification

Unfortunately, attackers are also keenly aware of the desire to get verified profiles and campaigns have cropped up targeting unsuspecting Instagram users.

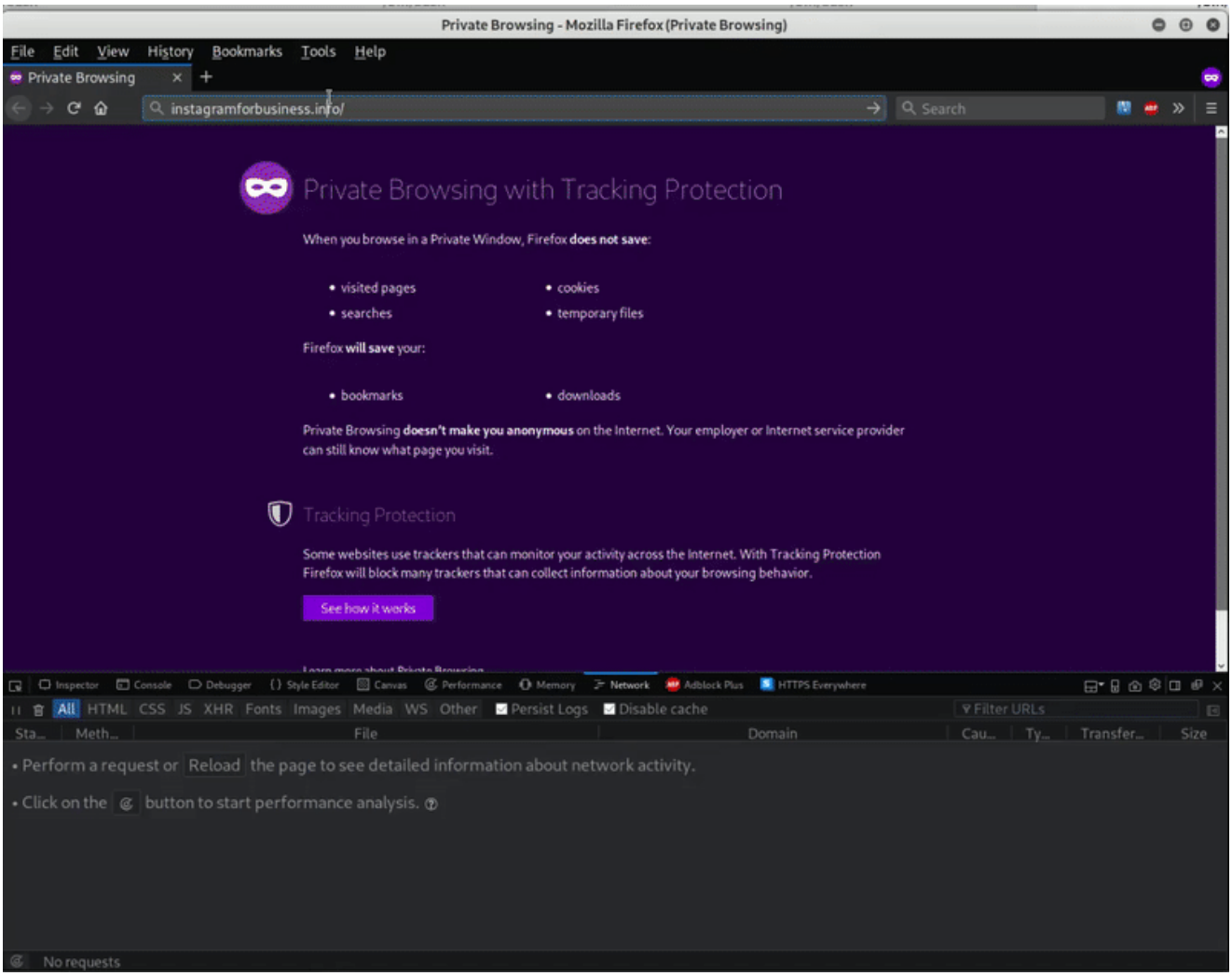
One clear example is this phishing page masquerading as the real Instagram Verification submission page:



Note the lack of SSL. This page also uses the **instagramforbusiness.info** domain, which *might* be mistaken for the legitimate **https://business.instagram.com/** page if a user isn't paying close attention.

Let’s take a look at what happens when an unsuspecting victim is lured into submitting their information to obtain a verified badge.

After clicking **Apply Now**, the page reveals a series of phishing forms on the domain **instagramforbusiness[.]info.**



This form targets the victim’s Instagram login information and then asks them to confirm their email address — by asking for their email address and password credentials. After each form submission, information is sent via email to the hackers which provides them with unauthorized access to the victim’s social media page.

Instagram employs fingerprinting and a variety of other methods to determine if an account login is suspicious. When suspicious activity is detected, they lock down the account with a **Suspicious Login Attempt** warning.

To circumnavigate this login attempt feature and avoid lockdown, attackers need **one** of the following pieces of information:

- Access to the **phone number** used to register the account (if applicable as Instagram doesn't require a phone number for signup)
- Access to the **email address** associated with the profile.

This explains why hackers target associated email login information on this phishing page; it allows them to reset and verify ownership of the phished Instagram account if the **Suspicious Login Attempt** warning is triggered.

Red Flags for Phishing & Scams

The lure of social media verification badges works great to entice unsuspecting victims. This is similar to the lure of "free" (i.e nulled, cracked) products like premium WordPress plugins or themes.

Don't let your situational awareness be lowered by the promise of an exclusive item or status, especially if it comes at a reduced cost. There are a number of red flags that this page was malicious:

- The domain name is clearly not **instagram.com**.
- Instagram will never ask for a linked email account's password as confirmation. It employs the standard method of sending verification links to the user's email.
- A lack of HTTPS results in insecure warnings in visitor's browsers. While you can't depend on SSL to determine if a site is trustworthy or not, large websites like Instagram typically display HTTPS — especially when handling login information and other sensitive information.

This domain has since been taken down, but it's a workflow that we see attackers regularly leveraging in their phishing campaigns.

Twitter Blue Badge Phishing

Users who've already obtained their verification badge aren't in the clear, either. Here's a recent example of password phishing targeting verified Twitter accounts for blue badge support.

> If you're a verified account and get this message from another verified account…..obviously….like don't. It's a password phishing scam. pic.twitter.com/2UTrNeUQU3
>
> — Sean Ross Sapp of Fightful.com (@SeanRossSapp) May 3, 2022

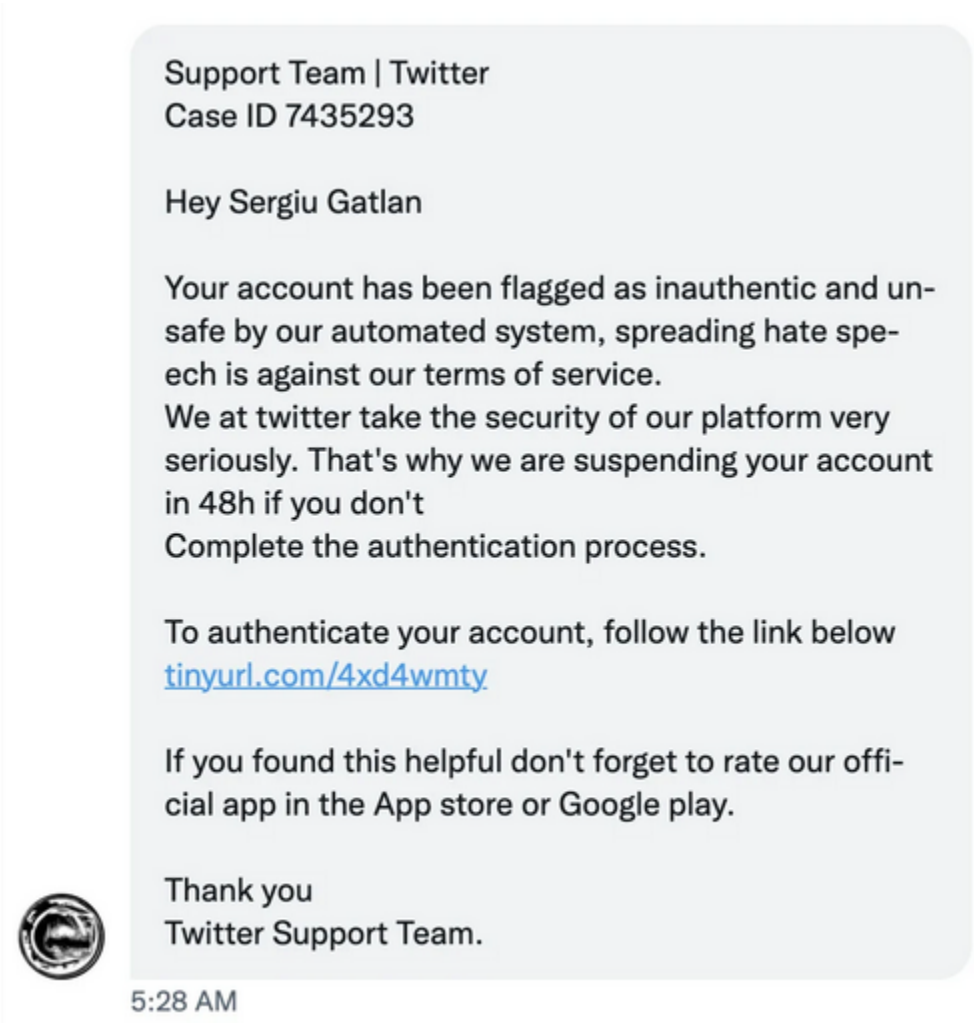
This DM, reported by SeanRossSapp, is made to appear authentic by leveraging the Twitter logo. Attackers include the corporate address at the bottom of the DM and make it appear as though it's being sent by an official **Blue Badge Support** account**.**

However, victims who follow the instructions and click on these malicious links are taken to a fake page designed to harvest and exfiltrate stolen account information to the attacker.

Twitter Account Suspension

Threats of account suspension can also lead unsuspecting victims into acting without thinking fully through a situation.

BleepingComputer reporter Sergiu Gatlan received a Twitter DM which claimed his account was breaching Twitter's terms of service and was under suspension for spreading hate speech.



Source: BleepingComputer and Sergiu Gatlan

As described in Sergiu's write-up, the tinyurl.com address in the DM redirects victims to a phishing landing page that leverages the Twitter API to check for valid credentials and pulls in user account images to add credibility to the scam.

These features found on more sophisticated phishing pages can make it challenging for even the most observant users.

How to protect your accounts

It's important to stay vigilant against social engineering attacks for all of your accounts — not just your website.

To avoid online scams and abuse for your social media accounts and beyond, here are some clear guidelines for you to follow.

1. Always check for suspicious URLs.

Exercise caution when clicking on links and verify that they're safe before you take any action.

2. Be wary of direct messages.

Social media services like Instagram and Twitter will never request log-in credentials via direct message.

3. Don't send personal details.

Never reveal personal information, provide selfies, or upload pictures of your personal identities to unsolicited users.

4. Ignore urgent requests.

Attackers often try to leverage urgent calls to action or threats in their phishing campaigns. Take a moment to pause and think about any requests you receive.

5. Avoid attachments and downloads.

Don't open attachments or download files from untrusted sources.

6. Be mindful that compromises can happen to your friends.

Your friends and acquaintances might not have their accounts on lockdown. So if you see a URL or request for information, don't assume it's safe just 'cause someone in your network sent it.

When in doubt, reach out to support for assistance. And always enable two factor authentication when possible — it may not prevent password change requests, but it will help prevent bad actors from gaining access to your accounts.

As a rule of thumb, always verify the links you are clicking on and ensure that you are only submitting personal information on legitimate websites. Malicious users are actively looking for a chance to deceive their victims with phishing campaigns. Stay safe online!