

CPF 000006-19-CID361-9H

27 March 2019



Typo and Squat More than an Office Exercise

We all know the cautionary tale about the wolf in sheep's clothing that tricks trusting children.

But, do you know the same story applies to the internet? There are cybercriminals who dress dangerous websites to look just like websites you are familiar with. Oftentimes a website you use frequently and trust.

The practice is known variously as spoofing, squatting, [cyber squatting](#) or [domain squatting](#), [typosquatting](#), and [website spoofing](#).

When accessing DoD websites, try a .mil web address first. While some DoD services have .com addresses, there is a recent example of a squatter using a DoD looking web address with a .com and victimizing one or more Soldiers. If you go to what should be a government or military site and the web address does not end in .gov, for government, or .mil, for military, be very cautious!

The names vary. The techniques vary. But, overall they are the cyber equivalent of a wolf in sheep's clothing.

Cyber Squatting

A cybercriminal squats when they create a website that has a slightly different web address than a legitimate one and they do so with intent to defraud. The squatter simply waits for someone to arrive at the fraudulent website.

You have your personal accounts at *MyBank*. You conduct your online banking at [www.MyBank.com](#). But in your haste, you do not notice that you type [www.MyBank.net](#). Or you did not notice the link you clicked on was [www.My-Bank.com](#).

Some businesses register multiple web addresses to reduce the potential dangers for customers.

[www.google.com](#), [www.google.net](#), and [www.google.info](#) lead to the same website.

And there are many other web addresses that lead to legitimate Google websites.

You know that [www.MyBank.net](#) and [www.My-Bank.com](#) are not the same as [www.MyBank.com](#). But you were in a hurry.

Fraudsters recognize this behavior and squat on an available web address that looks like a legitimate web address. Then they simply wait for you to arrive.

The website looks astonishingly like the genuine website. You log in to what you believe is your *MyBank* account. Maybe you see a message telling you the site is down and you are told to try again later. Maybe you see a message indicating you incorrectly entered your credentials and need to reenter them.

Contact Information:

Cyber Criminal Intelligence Program

27130 Telegraph Road

Quantico, Virginia 22134

Phone: 571.305.4482 IDSN 2401

Fax: 571.305.4189 IDSN 2401

Email

CCIU Web Page

CID LOOK OUT
ON POINT FOR THE ARMY

DISTRIBUTION:

This document is authorized for the widest release without restriction.



Protective Measures

- Be suspicious of any website or email with bad grammar, incorrect word usage, incomplete sentences or misspellings. All are indications the email or website is a fraud.
- Install, update and use a reputable antivirus product. DoD employees can download a free antivirus product from [Defense Information Systems Agency](#) using their Common Access Cards.
- Remember, regardless of which antivirus, anti-malware or network security software you use, no one will call you to tell you your computer is under attack.
- Rely on your bookmarks to access your most frequently visited websites. They are the most reliable. You decided to make them bookmarks. You decided they are reliable.
- Avoid clicking links you receive in emails and other sources if you already have the site bookmarked or if the email is from a source you do not recognize.
- Hover over the link before clicking and look along the bottom of your browser for the actual link to be revealed. The clickable link in the email could take you to an entirely different website (see insert).
- If you receive an email from a business or visit a website that has misspellings, incorrect punctuation, poor grammar or incorrect word usage, be very skeptical – very, very skeptical. This applies to both squatting and foreign language character substitution.
- If you suspect your login credentials have been compromised, change your passwords on the affected sites – as soon as possible and contact the website owner – and change passwords on other important sites, like financials, health and sites that contain your personal identifying information.

Resources

- [How Can I Identify a Phishing Website or Email?](#) – Yahoo.com
- [Recognize Suspicious Email & Websites](#) – Intuit Online Security
- [Examples of Links that Lie](#) – Horowitz Report
- [How to Spot and Avoid Tech Support Scams](#) – FTC.gov
- [Tech Support Scammers Using New Techniques](#) – ZDNet
- [Watch Out for Fake DoD Websites](#) – Military Times

To receive future CCIU Cybercrime Prevention Flyers, send an email to: usarmy.cciuintel@mail.mil with "SUBSCRIBE: CPF" in the subject line.



CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.