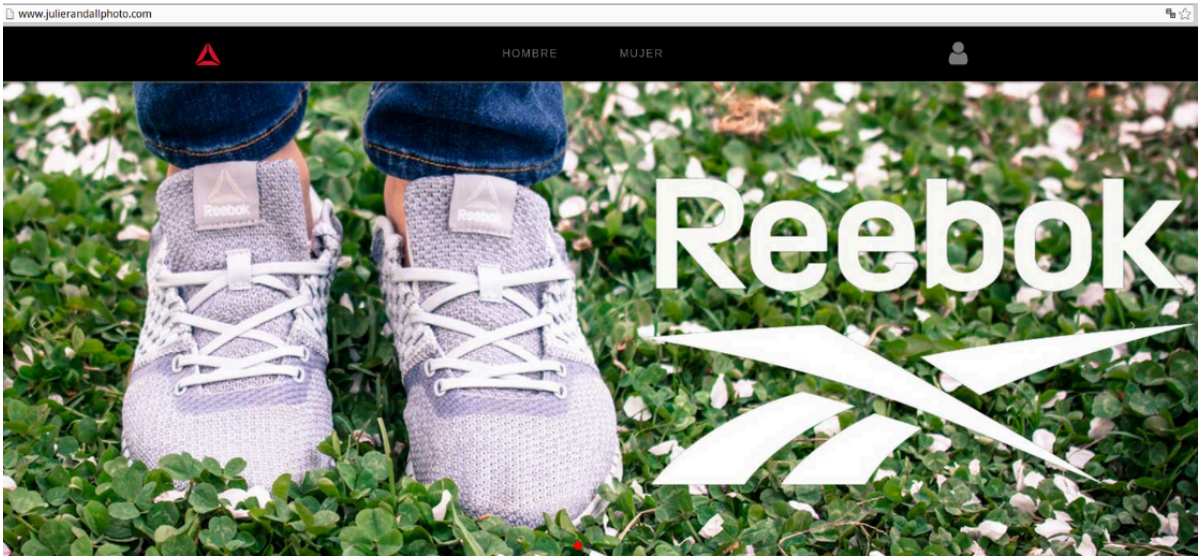
That Domain You Forgot to Renew? Yeah, it's Now Stealing Credit Cards

Published: 2018-11-13 · Archived: 2026-04-06 01:17:32 UTC

If you own a domain name that gets decent traffic and you fail to pay its annual renewal fee, chances are this mistake will be costly for you and for others. Lately, neglected domains have been getting scooped up by crooks who use them to set up fake e-commerce sites that steal credit card details from unwary shoppers.

For nearly 10 years, Portland, Ore. resident **Julie Randall** posted pictures for her photography business at **julierandallphoto-dot-com**, and used an email address at that domain to communicate with clients. The domain was on auto-renew for most of that time, but a change in her credit card details required her to update her records at the domain registrar — a task Randall says she now regrets putting off.



Julierandallphoto-dot-com is now one of hundreds of fake ecommerce sites set up to steal credit card details.

That's because in June of this year the domain expired, and control over her site went to someone who purchased it soon after. Randall said she didn't notice at the time because she was in the middle of switching careers, didn't have any active photography clients, and had gotten out of the habit of checking that email account.

Randall said she only realized she'd lost her domain after failing repeatedly to log in to her **Instagram** account, which was registered to an email address at julierandallphoto-dot-com.

"When I tried to reset the account password through Instagram's procedure, I could see that the email address on the account had been changed to a .ru email," Randall told KrebsOnSecurity. "I still don't have access to it because I don't have access to the email account tied to my old domain. It feels a little bit like the last ten years of my life have kind of been taken away."

Visit julierandallphoto.com today and you'll see a Spanish language site selling **Reebok** shoes (screenshot above). The site certainly looks like a real e-commerce shop; it has plenty of product pages and images, and of course a shopping cart. But the site is noticeably devoid of any SSL certificate (the entire site is http://, not https://), and the products for sale are all advertised for roughly half their normal cost.

A review of the neighboring domains that reside at Internet addresses adjacent to julierandallphoto-dot-com (**196.196.152/153.x**, etc.) shows hundreds of other domains that were apparently registered upon expiration over the past few months and which now feature similar http-only online shops in various languages pimping low-priced, name brand shoes and other clothing.

Until earlier this year, **wildcatgroomers-dot-com** belonged to a company in Wisconsin that sold equipment for grooming snowmobile trails. It's now advertising running shoes. Likewise, **kavanaghsirishpub-dot-com** corresponded to a pub and restaurant in Tennessee until mid-2018; now it's pretending to sell cheap **Nike** shoes.

So what's going here?

According to an in-depth report jointly released today by security firms **Flashpoint** and **RiskIQ**, the sites are almost certainly set up simply to siphon payment card data from unwary shoppers looking for specific designer footwear and other clothing at bargain basement prices.

"We have observed more than 800 sites hosting these brand impersonation/skimming stores since June 2018," the report notes.

"This group's strategy appears rather simple: the perpetrators set up a large number of stores impersonating as many popular brands as possible and drive traffic to these fake stores with a variety of methods," the report continues. "Some visitors will attempt to make purchases, entering their payment information into the payment form where the skimmer copies it and sends it to a drop server. The payment page even displays badges from various security companies in order to appear more legitimate."

The report tracks the work of **Magecart** — the name given to a collective of at least seven cybercrime groups involved in hacking Web sites to steal payment card data. On Nov. 4, KrebsOnSecurity published Who's in Your Online Shopping Cart?, which looked at a network of hacked sites that fit the Magecart profile.

Credit card data stolen by these various Magecart groups invariably gets put up for sale at online cybercrime shops, the security firms found. In addition, some Magecart actors will sell access to hacked online stores, allowing crooks who buy this access to receive a live feed of freshly-stolen payment card details for as long as the site remains compromised.

Flashpoint and RiskIQ say they have been working with two other non-commercial anti-abuse organizations, Abuse.ch and Shadowserver to "sinkhole" or quietly assume control over hacked domains that are used for Magecart activities. These latter two organizations provide automated reporting to affected organizations. Anyone responsible for managing a range of Internet addresses can sign up at Shadowserver.org to have those ranges monitored for domains compromised by Magecart tools.

Meanwhile, as Julie Randall's experience shows, it pays to stay on top of any domain registrations you may have. Giving up on a long-held domain name — particularly one tied to your name — is always a tough call, because

you simply never know what it will be used for when it falls into someone else's hands.

If you're on the fence about whether to renew a domain and it's one of several you own, it may make sense to hold onto it and simply forward any incoming traffic to a domain you do want people to visit. In the event you decide to relinquish a domain, make sure you take stock of any online accounts you created with email addresses tied to that domain and move those to another email address, as those accounts will likely come under someone else's control when the domain expires.
