

AttackSpotlight



SCAMMERS CREATE LOOKALIKE SITES TO TRICK WEB USERS

Stolen brand names, copied logos and https make dangerous websites seem safe

There are very few restrictions around naming a website. Virtually anyone can purchase an available web domain and use it for their own purposes.

Honest individuals and businesses own most website names. However, scammers frequently register domain names for malicious purposes. And they often choose names that include or resemble trusted brands in order to fool people. Our research shows that:

- 96% of organizations found exact matches of their website name with a different domain name ending—for example, “.net” vs. “.com”
- 85% of retail brands found websites selling counterfeit goods
- 76% of organizations found “lookalike” websites posing as their real websites

Phishing messages, social media posts and digital ads can contain lookalike links. Scammers might even copy your own organization’s name and brand.



What is a domain?

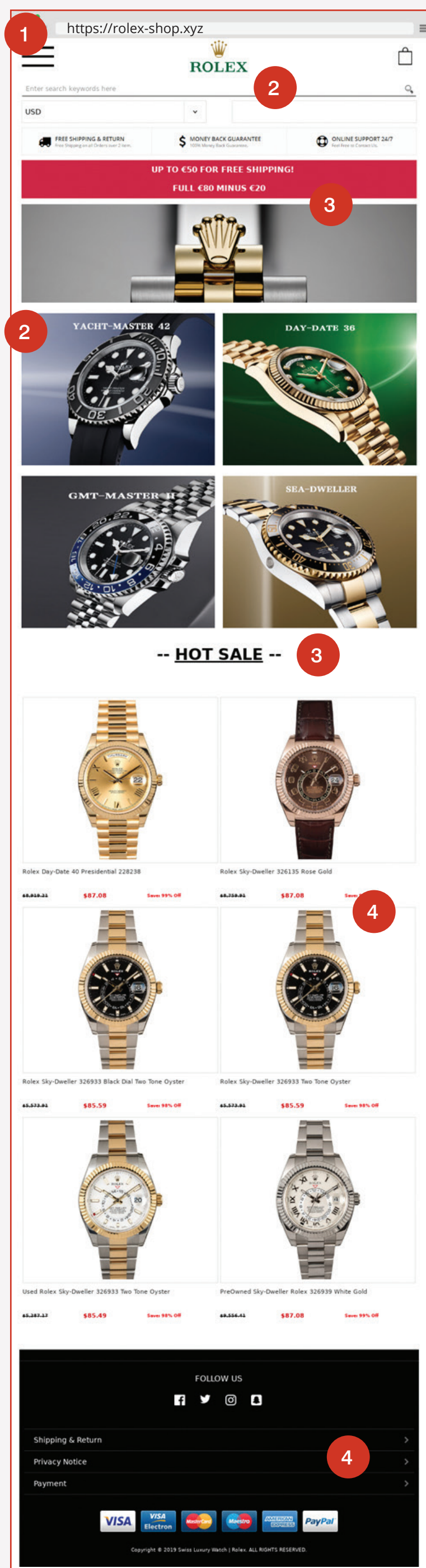
A domain is essentially the name of a website. Examples of domains include proofpoint.com, google.com, and amazon.com. Common domain name endings include .com, .net, and .org. But there are many more domain name endings, like .co, .top, .us, .xyz, and even .coffee.

Attackers who use fraudulent domains might try to:

- Sell you counterfeit goods
- Trick you into logging into a lookalike site in order to steal your password for the real site
- Steal your money or your organization’s money
- Fool you into downloading dangerous software like a virus or ransomware

WHAT SHOULD YOU LOOK FOR?

Scammers are very tricky and very creative. Below is an example of an actual lookalike website seen by Proofpoint researchers. (The website name, rolex-shop.xyz, has been changed slightly for your safety.) It mimics the real Rolex site and aims to sell counterfeit goods (or steal money). The tactics used on this site are commonly used on other lookalike sites.



- 1 The domain includes the real brand name. The site also shows “https” to indicate support for secure communications.
- 2 The site uses the real Rolex logo, and pictures and names of actual Rolex watch styles.
- 3 The lookalike site promises discounts, free shipping and a “hot sale.” This is not found on the real site.
- 4 The counterfeit site differs from the real Rolex site in an important way: **You cannot buy a watch through the real Rolex site.** The FAQ at Rolex.com says, “New and genuine Rolex watches are exclusively sold by Official Rolex Retailers.”

Anyone who purchases from the lookalike site would receive a counterfeit product—or lose their money and receive nothing at all.

HOW TO PROTECT YOURSELF

Do not take things at face value. Use these tips to identify dangerous and counterfeit sites:

- Avoid things that seem **too good to be true**. Do not trust websites, emails and ads that offer products and services at unusually low prices.
- Remember that **logos, brand names and pictures can be copied**. They do not prove that a site, link, email or ad is safe.
- Don’t confuse a “secure” site with a “safe” site. **Many cybercriminals buy security certificates for their websites**. That lets them use https and other indications of secure communications. **These visual cues are not proof the site is safe.**
- Stick with sites you know are safe when shopping online. **When in doubt, don’t check it out.**
- Only use personal devices (**not work-issued devices**) for personal activities.

Keep these tips in mind anytime you are browsing the web, not just when shopping online. Be sure to report suspicious websites and emails to your security team. And stay on the lookout for websites and links that mimic your organization’s brand.