I

Internationalized Domain Names (IDN): Punycode and Spoofing Risks

Internationalized domain names let people use native scripts in web addresses. Punycode is their DNS-compatible encoding, not evidence that a domain is malicious.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

An **internationalized domain name (IDN)** contains characters beyond basic ASCII, allowing people to use writing systems such as Arabic, Cyrillic, Chinese, Devanagari, and accented Latin in domain labels. IDNs make the web more accessible and are not inherently suspicious.

DNS still needs an ASCII-compatible representation. Software therefore uses an encoding called **Punycode** within the IDNA framework. An encoded label normally begins with `xn--`. Seeing that prefix means the label was encoded; it does not, by itself, mean phishing or malware.

How IDN and Punycode work

1. A user enters or follows a domain containing Unicode characters.
2. The browser processes each internationalized label according to IDNA rules.

3. DNS receives the ASCII-compatible form, while the browser may display either Unicode or Punycode.
4. The registry's registration policy and the browser's display policy provide separate layers of protection.

The W3C provides an accessible overview of multilingual web addresses. Display behavior differs between browsers, languages, and character combinations, so users should not rely on one expected visual warning.

What is an IDN homograph attack?

A homograph or homoglyph attack registers a different domain whose characters look like those in a trusted name. A Cyrillic character may resemble a Latin letter, but the code point and domain are different. Mixed-script labels are one pattern; a whole label written in another script can also be confusable. Ordinary ASCII domains such as `brand-login.example` can impersonate a company too, so IDN filtering cannot stop all look-alike attacks.

Unicode's current UTS #39 security mechanisms describe mixed-script and whole-script confusable detection. Even these tests produce legitimate matches and must be combined with context.

How to verify a suspicious domain

1. **Pause before signing in or paying.** Open the service from a saved bookmark, official app, or independently found contact page.
2. **Read the full hostname right to left.** Identify the registered domain immediately before the public suffix; text added farther left may only be a deceptive subdomain.
3. **Inspect the encoded form.** Copy the hostname into a trusted IDN/Punycode inspection tool, but treat the result as information rather than a verdict.
4. **Check provenance.** Compare the domain with the address published by the organization, including spelling, script, and top-level domain.

5. **Do not trust the padlock alone.** HTTPS protects the connection to the domain shown; it does not prove that the domain belongs to the brand it resembles.

If you used a look-alike site

Close the page without downloading anything. If credentials were entered, change them from the real service reached independently, revoke active sessions, review MFA and recovery settings, and change any reused password. Contact the bank through a known number if payment information was submitted. Scan the device if a file, extension, profile, or app was installed.

Defenses for organizations

- register important brand variants where risk and policy justify it;
- monitor newly registered confusable domains and certificate transparency data;
- use email authentication, web filtering, and phishing-resistant MFA;
- show users the exact official domains in onboarding and incident messages;
- report abuse to the registrar, hosting provider, browser protection services, and relevant authorities with supporting evidence.

IDN FAQ

Is every `xn--` domain unsafe?

No. It is the normal encoded form of an internationalized label. Judge ownership, context, and behavior.

Can a certificate prove a domain is the real brand?

No. A certificate can validate control of a domain and encrypt traffic while the domain itself is deceptive.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com