

# Ataques Homográficos y Ataques de Punycode

*“Si el dominio puede engañar a tu cerebro, puede engañar a tu contraseña.”*

Los **Ataques Homográficos** (o *Homograph Attacks*) son una forma de engaño visual diseñada para confundir a los usuarios al hacerles creer que están visitando un sitio web legítimo cuando, en realidad, están siendo dirigidos a una página fraudulenta controlada por un atacante.

Esta técnica explota la similitud visual entre caracteres de diferentes alfabetos o codificaciones. Los **Ataques de Punycode** son la manifestación técnica más común y efectiva de los ataques homográficos en el contexto de los nombres de dominio internacionales (IDN).

## ¿Qué es un Ataque Homográfico?

Un ataque homográfico se basa en el concepto de **homógrafo**, que es una palabra que se escribe igual que otra, pero tiene un significado diferente (aunque en ciberseguridad se refiere a caracteres que *parecen iguales*).

El atacante registra un nombre de dominio que visualmente es casi idéntico a una URL de una marca o servicio conocido.

## Tipos Comunes de Homógrafos

- **Diferentes Alfabetos (El Ataque de Punycode):** Se reemplazan caracteres latinos (como la 'a', 'o', 'e') por caracteres que se ven idénticos, o casi idénticos, de otros alfabetos, como el cirílico, el griego o el armenio. Este es el tipo más peligroso y se gestiona mediante Punycode.
- **Sustitución de Caracteres Similares:** Se reemplaza un carácter por otro que es similar en el alfabeto latino. Por ejemplo:
  - Reemplazar la letra minúscula 'l' (ele) por el número '1' (uno).

- Reemplazar la letra mayúscula 'O' por el número '0' (cero).
- Reemplazar la letra minúscula 'o' por el carácter griego 'ο' (ómicron).

### Ejemplo de URL Homográfica (Sustitución):

URL Legítima	URL Maliciosa (Homográfica)	Carácter Sustituido
amazon.com	amaz0n.com	'o' por '0'
p**a**ypal.com	p**a**ypal.com	'a' latina por 'a' cirílica

### ¿Qué es Punycode y Cómo Facilita el Ataque?

**Punycode** es un estándar de codificación que permite representar nombres de dominio que contienen caracteres no ASCII (es decir, caracteres fuera del alfabeto inglés básico, como acentos, diéresis, caracteres cirílicos, etc.) utilizando únicamente los caracteres ASCII permitidos. Punycode es esencial para la existencia de los **Nombres de Dominio Internacionalizados (IDN)**.

### El Funcionamiento de Punycode

Cuando un usuario quiere registrar un dominio como miñaña.com, el sistema de nombres de dominio (DNS) no puede procesar la ñ. Punycode convierte esta URL en una cadena de caracteres ASCII que el DNS puede entender.

- **Prefijo:** Todos los dominios codificados con Punycode comienzan con el prefijo `xn--`.
- **Codificación:** Punycode toma los caracteres especiales, los codifica y los añade al final del prefijo.

### Ejemplo de Punycode (Legítimo):

Nombre de Dominio (Visible)	Nombre de Dominio (Codificado por Punycode)
español.com	xn--espaol-zwa.com

### El Ataque de Punycode (IDN Homograph Attack)

El atacante utiliza Punycode para registrar un dominio que, cuando el navegador lo muestra, **parece idéntico** al dominio objetivo.

- Registro:** El atacante registra un dominio Punycode, por ejemplo, xn--pple-43a.com (que usa la 'p' cirílica).
- Visualización:** Cuando un navegador moderno soporta caracteres cirílicos, al encontrarse con xn--pple-43a.com, lo decodifica y lo muestra al usuario como apple.com.
- Engaño:** El usuario ve apple.com en la barra de direcciones, asume que está en el sitio legítimo, e introduce sus credenciales.

### Ejemplo de URL Homográfica con Punycode (Malicioso):

URL Objetivo (Legítima)	Cadena Maliciosa de Punycode	URL Decodificada (Engaño Visual)
apple.com	xn--pple-43a.com	apple.com
google.com	xn--gogle-8rb.com	google.com
bankia.es	xn--bnkia-jxa.es	bankia.es

### Ejemplos de Ataques Reales

El ataque de Punycode es una amenaza constante y ha sido utilizado para suplantar a algunas de las marcas más grandes del mundo.

#### 1. Falsificación de Apple (2017)

- Contexto:** Uno de los ejemplos más notables fue un ataque de Punycode que utilizaba un certificado SSL válido para hacer

que un dominio malicioso se viera idéntico a apple.com en la barra de direcciones de Chrome y Firefox.

- **Mecanismo:** El dominio utilizado era, por ejemplo, xn--80ak6aa92e.com (que decodificado en algunos navegadores se veía como **apple.com**). El atacante pudo obtener un certificado SSL/TLS (el candado verde) para el dominio Punycode, lo que aumentaba la sensación de legitimidad para el usuario.

## 2. Engaño de Steam (2017)

- **Contexto:** La plataforma de videojuegos Steam fue atacada con un esquema de *phishing* de Punycode. Los atacantes creaban URLs que parecían provenir de la comunidad de Steam.
- **Resultado:** Usuarios que accedían a estos enlaces eran dirigidos a sitios de *Login* falsos donde se robaban sus credenciales y, potencialmente, el acceso a sus bibliotecas de juegos.

## Medidas de Protección y Mitigación

Para protegerse de estos ataques, tanto usuarios como desarrolladores y navegadores han tomado medidas:

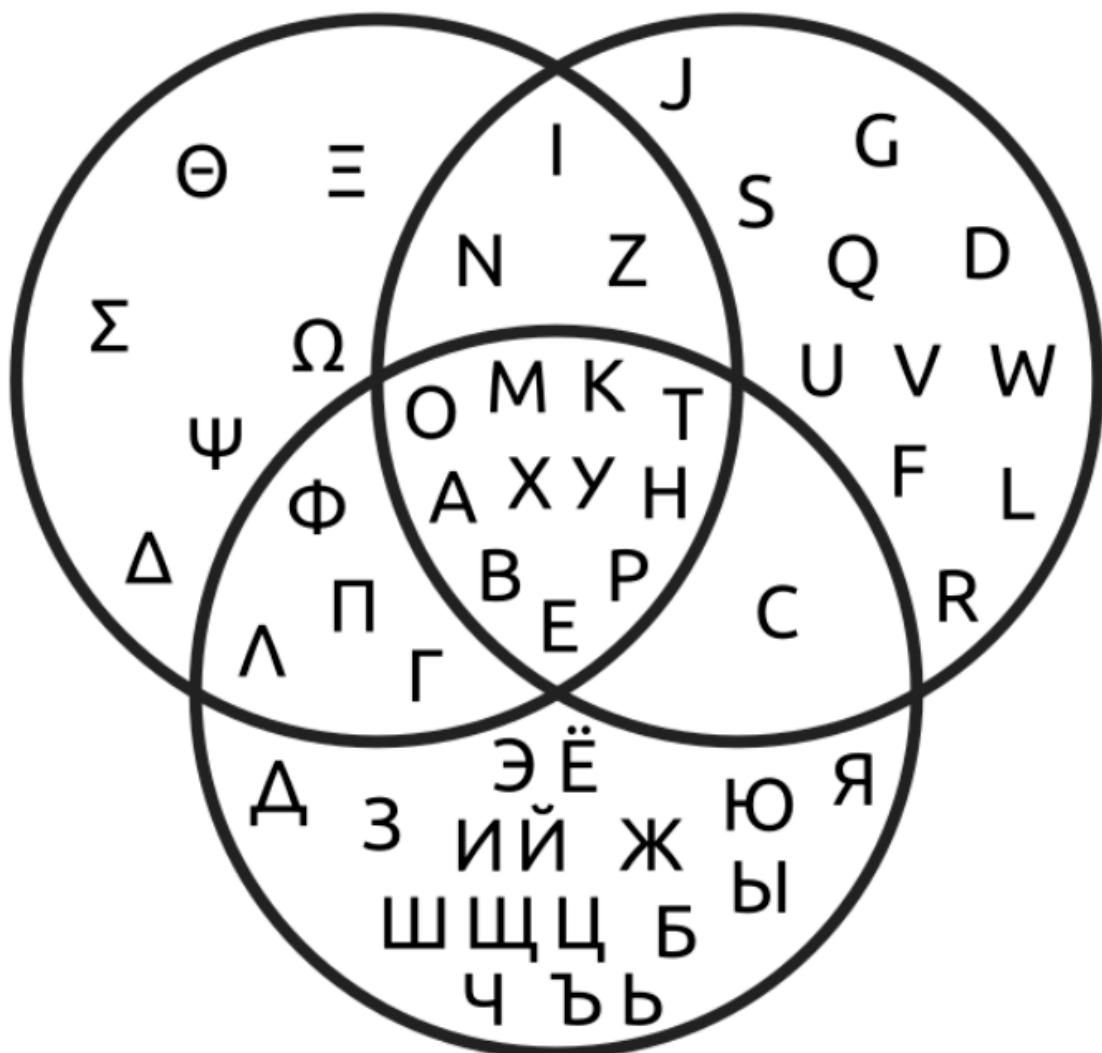
### Para Usuarios

- **Inspección Detallada de la URL:** Presta especial atención a la barra de direcciones, incluso si ves el candado de seguridad (HTTPS). Si la URL se ve sospechosa, cópiala y pégala en un conversor de Punycode *online* para ver si tiene el prefijo xn--.
- **Utilizar Administradores de Contraseñas:** Los gestores de contraseñas (*password managers*) solo autocompletarán las credenciales si el dominio coincide **exactamente** con el dominio legítimo. El dominio Punycode no coincidirá con el dominio legítimo, por lo que el gestor no actuará.
- **Verificar el Certificado:** En la barra de direcciones, haz clic en el candado para ver el certificado de seguridad. Un navegador moderno podría mostrar el nombre Punycode real del dominio en la información del certificado, lo que revelaría el engaño.

## Para Navegadores y Desarrolladores

- **Bloqueo Heurístico:** La mayoría de los navegadores modernos (Chrome, Firefox, Edge) han implementado heurísticas avanzadas para mitigar estos ataques. Por ejemplo, si una URL utiliza una mezcla de alfabetos (Latino y Cirílico), el navegador puede optar por mostrar la versión codificada con Punycode (xn--...) en lugar de la versión decodificada visualmente, rompiendo así el engaño.
  - **Registro Proactivo:** Las grandes marcas pueden registrar dominios Punycode que sean visualmente idénticos a su propia marca (registros defensivos) para evitar que los atacantes los utilicen.

*Diagrama de Venn de Letras superpuestas en alfabetos europeos (Latino, griego y cirílico):*



**Tabla de ejemplos de ataques homográficos / Punycode**

Dominio visual (Unicode)	Dominio legítimo	Carácter engañoso	Código Unicode	Dominio Punycode	Tipo
appIe.com	apple.com	a p p I e (cirílico)	U+0430 U+0440 U+0440 U+04CF U+0435	xn--80ak6aa92e.com	IDN homograph puro
apple.com	apple.com	a (cirílico)	U+0430	xn--pple-43d.com	Sustitución parcial
google.com	google.com	e (cirílico)	U+0435	xn--googl-r7a.com	Sustitución parcial
microsoft.com	microsoft.com	o (cirílico)	U+043E	xn--microsf-n0g.com	Sustitución parcial
paypal.com	paypal.com	p a (cirílico)	U+0440 U+0430	xn--ypal-43d.com	Phishing bancario
twitter.com	twitter.com	w (griego)	U+03C9	xn--titter-i2e.com	Homoglyph griego
facebook.com	facebook.com	a (cirílico)	U+0430	xn--fcebook-43d.com	Ingeniería social
instagram.com	instagram.com	a (cirílico)	U+0430	xn--instgram-43d.com	Phishing social
gm&il.com	gmail.com	a (latino con diacrítico)	U+1EA1	xn--gmil-6q5a.com	Diacríticos
youtube.com	youtube.com	т (cirílico)	U+0442	xn--youube-4fg.com	Sustitución parcial
amazon.com	amazon.com	a (cirílico)	U+0430	xn--mazon-43d.com	Comercio electrónico
linkedin.com	linkedin.com	. (punto Unicode)	U+2024	xn--linkedin-m2f.com	Separador falso

## Ejemplo explicado paso a paso

Ejemplo: google.com

Lo que ve el usuario:

google.com

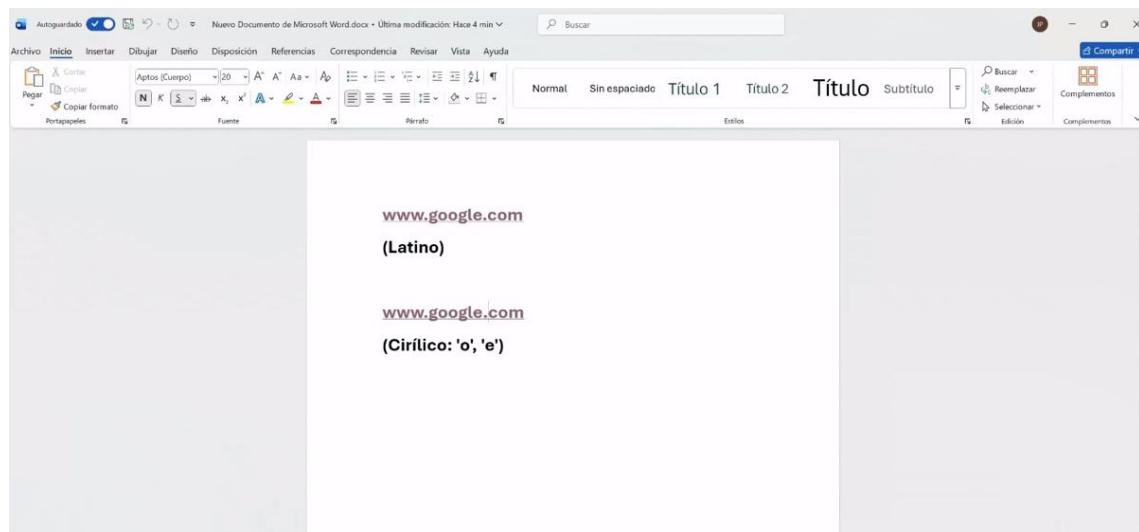
Lo que realmente es:

- La última “e” no es ASCII
- Es la letra cirílica e (U+0435)

Conversión real (DNS):

xn--googl-r7a.com

El navegador puede mostrar google.com visualmente, pero el dominio no pertenece a Google.



## Resumen visual de caracteres más usados en ataques

Carácter visual	Unicode	Escritura	Sustituye a
a	U+0430	Cirílico	a
e	U+0435	Cirílico	e
o	U+043E	Cirílico	o
p	U+0440	Cirílico	p
c	U+0441	Cirílico	c
т	U+0442	Cirílico	t
ѡ	U+03C9	Griego	w
ã	U+1EA1	Latino	a
.	U+2024	Unicode	.

## Ataques de phishing basados en similitud visual de dominios

### 1) Dos grandes familias de ataques visuales en phishing

#### A. Ataques homográficos Unicode / Punycode

- Usan caracteres Unicode (cirílico, griego, etc.).
- Ejemplo: microsoft.com (la “o” es cirílica).
- El dominio real es xn--microsoft-n0g.com.

#### B. Ataques ASCII look-alike (tipográficos)

- NO usan Unicode
- Usan combinaciones de letras ASCII visualmente parecidas.
- Ejemplo clásico:  
rnicrosoft.com → parece microsoft.com
- Son mucho más difíciles de detectar para usuarios y filtros automáticos.

**Importante:**

`rnicrosoft.com` NO es Punycode, NO es IDN, y NO empieza por `xn--`. Es un ataque puramente visual + psicológico, muy usado en phishing real.

**2) Ejemplo clave: `rnicrosoft.com`**

**¿Por qué funciona?**

- La letra `m` en muchas tipografías se parece a `n`
  - En emails, móviles y tipografías pequeñas:
    - `rnicrosoft.com`
    - `microsoft.com`
- visualmente casi indistinguibles

**Tipo de ataque**

Característica	Valor
Tipo	Phishing ASCII (no Unicode)
Técnica	Homoglifo tipográfico
Defensa por Punycode	✗ No aplica
Riesgo	🔥 Muy alto

**Uso típico**

- Correos de “Seguridad de Microsoft”
- Alertas falsas de cuenta bloqueada
- Páginas falsas de login Microsoft 365 / Outlook

**3) Tabla ampliada: dominios de phishing visualmente casi idénticos**

### A) Ataques ASCII (sin Unicode) – los más peligrosos

Dominio falso	Dominio real	Engaño visual	Tipo
rnicrosoft.com	microsoft.com	rn → m	Phishing corporativo
paypaI.com	paypal.com	I mayúscula → l	Bancario
faceb00k.com	facebook.com	00 → oo	Redes sociales
gmaiI.com	gmail.com	I → l	Robo de correo
micros0ft.com	microsoft.com	0 → o	Malware / phishing
arnazon.com	amazon.com	rn → m	Comercio
l1nkedin.com	linkedin.com	l1 → li	Ingeniería social

- Todos estos dominios son 100% ASCII válidos
- Pueden tener HTTPS legítimo
- No disparan alertas IDN

### B) Ataques Unicode / Punycode (homográficos clásicos)

Dominio visual	Dominio real	Carácter falso	Unicode	Punycode
microsoft.com	microsoft.com	o cirílica	U+043E	xn--microsoft-n0g.com
appIe.com	apple.com	cirílico	varios	xn--80ak6aa92e.com
google.com	google.com	e cirílica	U+0435	xn--googl-r7a.com
paypal.com	paypal.com	p a cirílicas	U+0440 U+0430	xn--ypal-43d.com

## 4) Escenario real de phishing (paso a paso)

Caso típico: Microsoft 365

- 1 Usuario recibe email:

Asunto: Actividad sospechosa en su cuenta Microsoft

- 2 Enlace visible:

<https://rnicrosoft.com/security-check>

- 3 Página clonada:

- Logo oficial
- Certificado HTTPS válido
- Diseño idéntico al login real

- 4 Usuario introduce credenciales

- 5 Credenciales enviadas al atacante

- 6 Acceso a correo, OneDrive, Teams, SharePoint

**Resultado:**

- Compromiso de cuenta
- Movimiento lateral en la empresa
- Fraude BEC (Business Email Compromise)

## 5) ¿Por qué estos ataques funcionan tan bien?

Factor	Impacto
Lectura rápida	El cerebro “corrige” automáticamente
Tipografías sans-serif	Ocultan diferencias
Pantallas pequeñas	Móvil = mayor riesgo
HTTPS	Falsa sensación de seguridad
Fatiga del usuario	Menos comprobaciones

## **6) Diferencia clave para explicar en formación**

**“HTTPS ≠ sitio legítimo”**

Un dominio como `rnicrosoft.com` puede tener:

- Certificado TLS válido
- Candado verde
- Dominio aparentemente correcto

Y aun así ser **100% malicioso.**

## **7) Medidas de defensa específicas contra phishing visual**

### **Para usuarios**

- Leer dominios **letra a letra**
- Desconfiar de `rn`, `lI`, `00`
- Acceder a servicios críticos **solo desde marcadores**
- Revisar dominio real en el certificado

### **Para empresas**

- Bloquear dominios look-alike (ASCII + Unicode)
- Registrar variantes defensivas (`rn`, `lI`, `00`)
- Formación específica en **homoglifos ASCII**
- MFA obligatorio (reduce impacto, no lo elimina)
- Monitorizar dominios similares al propio

maybank2u.com is not the same as  
maybank2u.com

citibank.com is not the same as  
citibank.com

(the first one is correct, the second one  
is from hackers)

The "a" in the later url is a cyrillic  
alphabet.

## ssword Reset Request



Microsoft <no-reply@microsoft.com>

To

rnicrosoft.com