

# GUARDIA CIVIL

## CONSEJOS PARA EVITAR ESTAFAS

- AL COMPRAR EN TIENDA FÍSICA

### 1. SU TARJETA CON USTED

NO ENTREGAR LA  
TARJETA A TERCEROS, sea  
SIEMPRE usted quien  
acerque o introduzca la  
tarjeta en el datáfono al  
pagar, EVITARÁ intentos  
de clonación.

### 2. SEA PRECAVIDO

Antes de teclear el  
número pin de la tarjeta  
de crédito en el datáfono  
o en un cajero,  
ASEGURARSE DE QUE  
NADIE ESTÁ  
OBSERVANDO.

### 3. CONTRASEÑA SIEMPRE

Si utiliza el teléfono para  
pagar, PÓNGALE  
CONTRASEÑA. Dificultará  
que alguien pueda  
acceder cuando usted no  
lo esté utilizado

# GUARDIA CIVIL

## CONSEJOS PARA EVITAR ESTAFAS

- AL COMPRAR EN INTERNET (COMERCIOS O ANUNCIOS DE PARTICULARES

### 1. CUIDADO CON LOS CHOLLOS

Con regalos, sorteos u ofertas con tiempo limitado expuestas EN REDES SOCIALES TIPO INSTAGRAM, FACEBOOK o páginas como WALLAPOP o MILANUNCIOS. Desconfíe de BAJADAS EXTREMAS DE PRECIO.

### 2. COMPRUEBE LA EXISTENCIA DEL PRODUCTO

En compras a particulares NUNCA INGRESE DINERO POR ADELANTADO sin antes haber visto el producto (ES UNA ESTAFA CLÁSICA)

### 3. NO CEDA A LAS PRISAS

Intentan QUE PIQUE diciéndole que se va a quedar sin el producto porque hay otros compradores o finaliza la oferta.

### 4. VERIFICAR LA DIRECCIÓN DE LA PÁGINA WEB

Compruebe SIEMPRE que la dirección de la página coincida EXACTAMENTE con la de la tienda, a veces varía en una simple vocal. LO IDEAL ES QUE LA ESCRIBA USTED EN LUGAR DE PINCHAR EN ENLACES.

### 5. DIRECCIÓN WEB CON HTTPS

La dirección de la página web SIEMPRE DEBE COMENZAR con "https" NO debe haber guiones u otros símbolos como http-s o que falte la "s" "http".

### 6. COMPRAR EN COMERCIOS SEGUROS

Antes de pagar, CONFIRMAR que la PÁGINA WEB es SEGURA. Puede comprobarlo por ejemplo en:

- <https://www.virustotal.com/>
- <https://app.webinspector.com/>
- <https://sitecheck.sucuri.net/>
- Norton Safe Web.

### 7. COMPRUEBE QUE ESTÁ EL CANDADO

Asegúrese de que la dirección de la página (URL) tiene el símbolo DEL CANDADO antes de https. (Este símbolo garantiza la encriptación de los datos y la autenticación de la página web)

### 8. MÉTODOS DE PAGO VARIADOS

Desconfíe si la página web solo tiene un método de pago. Debe tener diferentes opciones para pagar (TRANSFERENCIA, MASTERCARD, VISA, PAYPAL, etc.) Si puede elija PAYPAL.

### 9. PÁGINAS FRAUDULENTAS

Desconfíe de las páginas con erratas, partes sin traducir, si no tienen datos de contacto claros u ofrecen un aspecto extraño. Compruebe que la web a la que se accede tiene apartado con información legal

# GUARDIA CIVIL

## CONSEJOS PARA EVITAR ESTAFAS

### OTROS CONSEJOS INTERESANTES

- Tenga un **ANTIVIRUS ACTUALIZADO** en su ordenador y en su móvil.
- Proteja **SIEMPRE CON CONTRASEÑAS** su teléfono, tablet u ordenador.
- **NUNCA DIGA SUS CLAVES O CONTRASEÑAS** por correo electrónico o teléfono, ni siquiera, aunque sea el banco el que le llama diciendo que es para evitar un **FRAUDE O PROBLEMA CON SU CUENTA. EL BANCO NUNCA LE PEDIRÁ LAS CLAVES POR TELÉFONO O CORREO ELECTRÓNICO.**
- **NUNCA** proporcione **FOTOCOPIAS** del DNI u otros documentos.
- Tampoco proporcione su número de tarjeta de crédito por teléfono a menos que esté completamente seguro de estar tratando con alguien de confianza.
- Si recibe una llamada en la que le piden datos personales. **CUELGUE Y DEVUELVA LA LLAMADA AL NÚMERO OFICIAL QUE FIGURA EN LA PÁGINA WEB DE LA ENTIDAD O EMPRESA QUE LE LLAMA.**
- **NO** guarde automáticamente los datos de su tarjeta.
- Elimine constantemente las "cookies" del navegador de internet para evitar el robo de credenciales.
- **NO CONFÍE** en correos electrónicos que cambian métodos de pago o cuentas. Si dicen ser de una compañía con la que usted tiene actividades comerciales, diríjase a su sitio web **O AL CONTACTO HABITUAL y COMPRUEBE.**
- Es recomendable utilizar una modalidad de pago seguro como **PAYPAL**, con el certificado **SSL**.
- Piénselo dos veces antes de compartir su información personal en redes sociales. Los estafadores recolectan información personal para hacerse pasar por sus víctimas.