

Key Insights

DolceVisa® is proud to help people with passport, visa, and travel document needs. But because we work in an area that involves sensitive information — such as identity documents, fees, and online payments — scammers sometimes pretend to be us.

We want you to be prepared. This means keeping up to code on how scammers operate, and attempt to scam you by pretending to be us.

3.4 Billion Phishing Emails are Sent Every Single Day (AAG)

This document explains exactly how to be protected, and what you can do.

Fake Links and Lookalike Characters

Scammers may attempt to pretend to be us by creating websites or links with very similar letters from different alphabets.

See the example below

dolcevisa.com → This is our official website **dolcevisa.com** → This uses the Cyrillic D

Potential Special Characters Used in Lookalike Attacks		
Letter	Common Substitutes	Notes
d	d (Cyrillic small letter), & (script), đ	Looks like lowercase 'd'
0	0 (zero), o (Greek omicron), ö (Cyrillic o with diaeresis)	Hard to spot difference
I	1 (one),	(pipe), ι (Latin iota), ł
С	c (Greek sigma), ċ (dot c), ċ	Subtle shape difference
е	e (Cyrillic e), ė, €	Cyrillic 'e' is visually identical
V	ν (Greek nu), ῦ	Almost indistinguishable in some fonts
i	1,	(pipe), ί, ι (Greek iota)
s	s (Cyrillic s), ș, \$	Common fake
а	a (Cyrillic a), α, à	Cyrillic 'a' is often used
.com	.com (Cyrillic 'o'), .com (Cyrillic 'c'), .com (Cyrillic c + Greek o)	Easy to spoof entire domain

The safest way to protect yourself against this is by typing the URL yourself, and not clicking the link.

Pretending to be us over the phone

Another way scammers contact you is by calling you. Scammers may pretend to be us, and request either

- Payment
- Confidential Document Numbers

See the example below



Scammers use a technique called "Sim Swapping" where, when they call, it will show DolceVisa's real phone number.

If you are concerned, please hang up and redial the number using the keypad (don't click from recents). When you dial, it will always come back directly to us.

Pretending to be us over the phone

Another way scammers contact you is by calling you. Scammers may pretend to be us, and request either

- Payment
- Confidential Document Numbers

We'll never ask for confidential information over the phone. If you are worried, please hang up, and redial this phone number:

02032399065

Just like before, if you enter the number manually, they cannot redirect it to them. Only when they call you can they "spoof" the number to make it seem like us.

Asking for Private Details

Scammers are innovating with how they do things, and we're likely to miss things. So, if **anything** seems off, hang up, close the email, close the tab, and call us immediately.

If anything seems off, like randomly being asked for certain details, always stop.

For example, if you suddenly get asked for a Passport Number, but you're currently not dealing with any passport details, it is most likely a scam.

Always call us if something seems off.