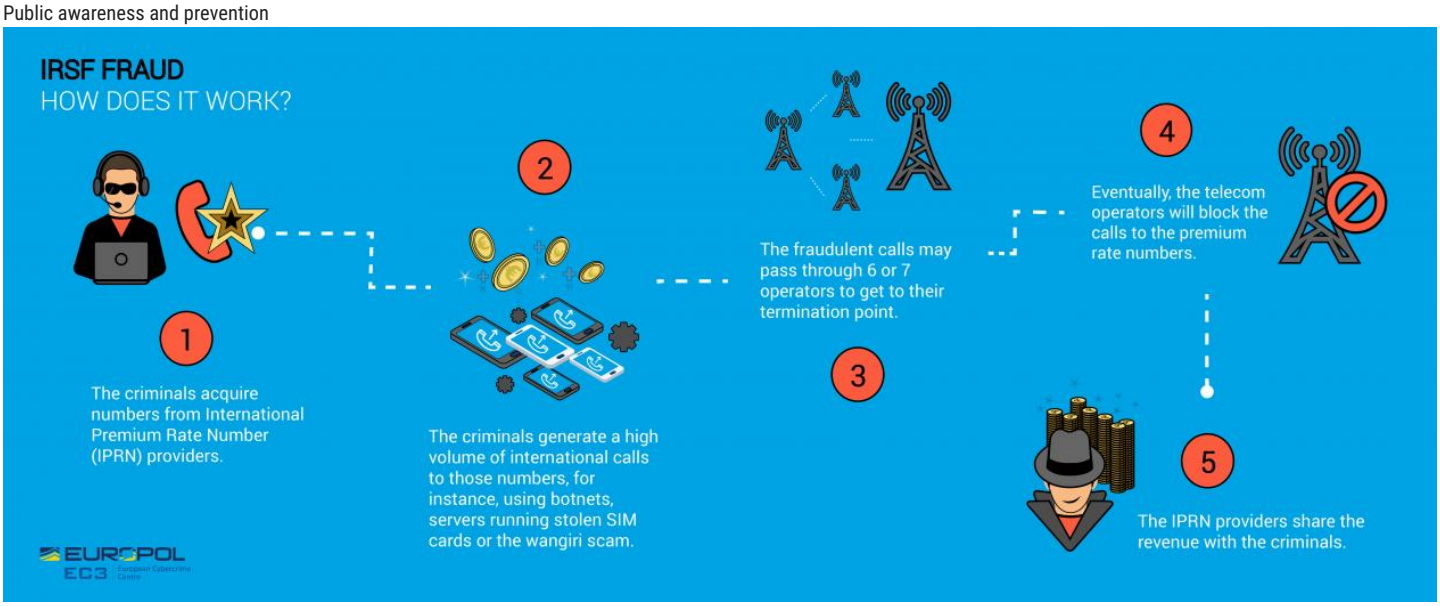
TELECOMMUNICATIONS FRAUD

Public awareness and prevention



Read the Cyber-Telecom report, jointly drafted with Trend Micro.

Telecommunications fraud (aka Telecom fraud) represents a serious threat to the telecommunication industry. It refers to the abuse of telecommunications products (mainly telephones and cell phones) or services with the intention of illegally acquiring money from a communication service provider or its customers.

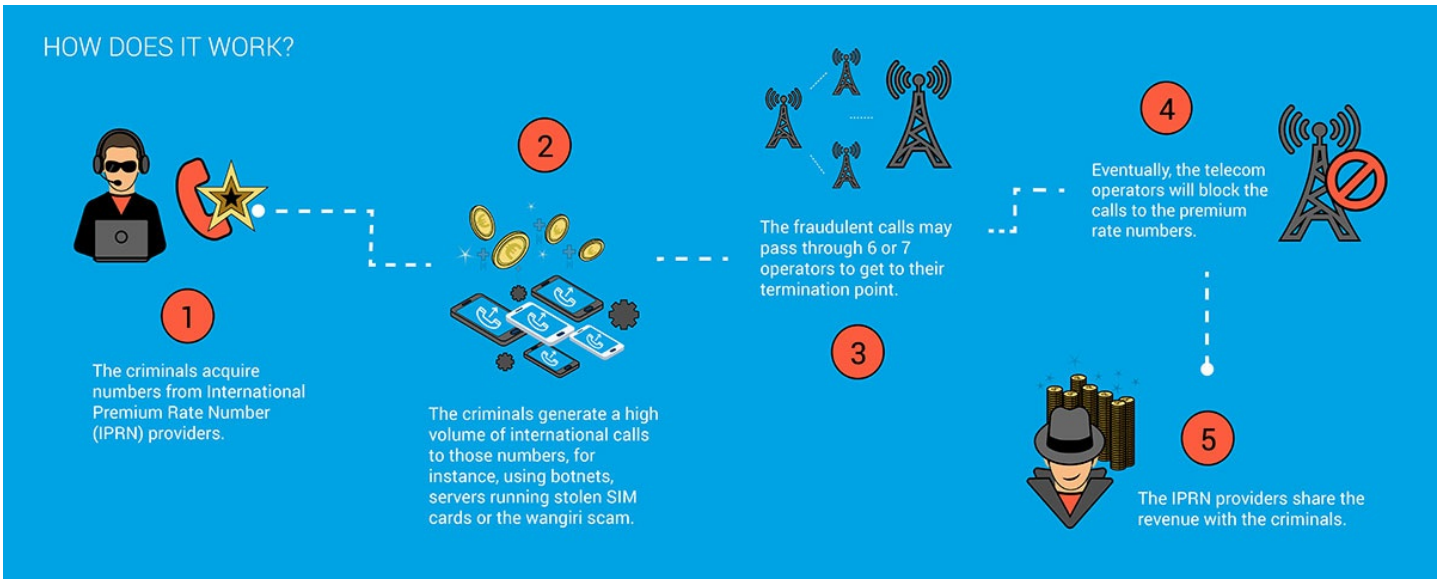
Telecom fraud can take many different forms, among others:

INTERNATIONAL REVENUE SHARING FRAUD (IRSF)

This is the most damaging fraud scheme to date, where a criminal partners with an International Premium Rate Number (IPRN) provider [1] that charges high rates for call termination and agrees to share revenue for any traffic generated by the fraudster.

IRSF is characterized by:

- High volume of international calls, often with long duration, to a single high-cost destination (countries outside of the EU).
- Some calls are automatically generated by the fraudsters (e.g. botnets and servers running stolen SIM cards). Some others are done by consumers (see Wangiri fraud below).
- The fraudulent calls may pass through 6 or 7 operators to get to their termination point.
- High revenue for the criminals obtained as a result of the inter-carrier trust between telecom operators. As there is no customer to bill because the connection is fraudulent, the originating operator has to pay and carry that loss.



This crime can have a significant impact on you, as customer, including:

- loss of connectivity due to being blocked at the carrier/telecom infrastructure level;
- prolonged outages while you justify to the carriers involved that you are the victim and not the perpetrator;
- extremely expensive phone bills.

[1]Not all International Premium Rate Number (IPRN) providers are fraudsters. There are legitimate operators offering genuine services.

One (ring) and cut – the Wangiri fraud

Download the Wangiri fraud infographic.

Wangiri is a Japanese word meaning 'one (ring) and cut'. It's a telephone scam where criminals trick you into calling premium rate numbers. A fraudster will set up a system (for instance using botnets) to dial a large number of random phone numbers. Each calls rings just once, then hangs up, leaving a missed call on the recipients' phone. Users often see the missed call and, believing it was a legitimate call, call back the missed number.

What are the signs? The call…

- takes place at night or during working hours (reducing the chances for the recipient to answer the call);
- rings only once;
- displays an unusual international country code.

What can you do?

- If you have a missed call from an unknown number, don't call back. A legitimate caller will either leave a message or call back.
- If you receive several such calls, let your phone operator know.

Vishing calls

Download Vishing calls infographic.

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters trick you into divulging your personal, financial or security information or into transferring money to them.

What can you do?

Attackers may use Caller ID Spoofing which makes it appear that they are calling from your bank, your government, a reputable private company, or a local number.

- Beware of unsolicited telephone calls.
- Take the caller's number and advise them that you will call them back.
- In order to validate their identity, look up the organisation's phone number and contact them directly.
- Don't validate the caller using the phone number they have given you (this could be a fake or spoofed number).
- Your personal details may be available online (e.g. on social media). Don't assume a caller is genuine just because they have such details.
- Don't share your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- Don't transfer money to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, report it to your bank and let your phone operator know.
- Block unknown and unwanted calls – ask your phone carrier about available blocking tools.

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES	European Cybercrime Center (EC3)