

Safe and sound

How you can protect yourself from crime

Your Police and the Swiss Crime Prevention – an office of the ministries of justice and police of the Cantons.

Editor

Swiss Crime Prevention (SCP)
House of Cantons
Speichergasse 6, Postfach, CH-3001 Bern
Responsible: Chantal Billaud
E-Mail: info@skppsc.ch, www.skppsc.ch

The brochure is available from every police office nationwide as well as from the police of the Principality of Liechtenstein.

It is edited in English (online only), German, French and Italian. Downloads are available from www.skppsc.ch.

Text

Volker Wienecke, Berne

Layout and illustration

Weber & Partner, Berne, www.weberundpartner.com

Copyright

Swiss Crime Prevention (SCP) April 2014, 1st edition

Safe and sound

How you can protect yourself from crime

Dear Readers	2
1. Violent crime	7
1.1. Domestic abuse	
1.2. Threatening behaviour	
1.3. Violent public order offences	
1.4. Vandalism	
1.5. (Cyber) bullying and mobbing	
1.6. Stalking	16
2. Sexual offences	19
2.1. Sexual assault and rape	
2.2. Paedophilic crime	
2.3. Illegal pornography and sexting	24
3. Internet-based offences	27
3.1. Internet-based fraud	
3.2. Phishing	
3.3. Hacking and malware	
3.4. Sextortion	36
4. Property crime	39
4.1. Theft	
4.2. Burglary	
4.3. Robbery	
4.4. Fraud	46
5. Weapons	50
6. Civic courage	52
Contact details of cantonal and municipal police forces	56

Dear Readers

"Prevention is better than cure", so goes the proverb, because experience has taught us that even a successful recovery can leave scars – and not just from illnesses and accidents. Being the victim of crime can also leave its mark.

Anyone who has been subject to a brutal mugging is bound to be wary in the future. Many of those who have experienced a burglary report that they no longer feel properly secure in their own home. And following a rape, in many cases even the best psychological support is unable fully to resolve the trauma that has occurred.

Of course, it would be better if such criminal acts never happened at all. Each and every one of us¹ can help to protect ourselves and those around us from crime. SKPPSC Swiss Crime Prevention raises the awareness of the general public – and thus of potential victims – about the possible dangers, and highlights the best ways of guarding against them. For advice, please refer to "What you should do" at the end of each section of this booklet.

The risks which can result in someone becoming a victim of crime are as broad and varied as life itself. What's more, in the age of rapidly advancing digitalisation, there is at least one new and virtual danger zone to match almost every conventional risk area from the analogue world. It's a never-

¹ This booklet uses gender-neutral language, except in cases in which it seemed appropriate for objective reasons to use one gender or the other. For example, the great majority of perpetrators of paedophilic crime are men, while romance scams primarily affect women.

ending story: no sooner have you got to grips with the latest app than there is a con artist on the other end of the line just waiting for you to fall into their trap.

Of course, there is plenty to discover from the infinite breadth of the internet: products and services of all kinds, information on any issue you can name, opinions and comments, fake news and conspiracy theories, friendship, love and sex, photos and films, games involving players from around the world, pornography and much more. Beware, however, that there is also plenty to lose: personal data, money, trust, hope, reputation – and face!

The fault lies with specific security loopholes which, for many reasons, make the internet the perfect setting for crime. Firstly, you can't immediately touch, examine and take home anything you see on the internet. In the first instance, everything remains **virtual**, based simply on what another person claims. Anyone who becomes emotionally, and then financially, invested in a person or an object is necessarily paying some form of advance which another party can simply take, without providing anything in return. Secondly, anyone making false claims on the internet is able to remain anonymous - and because of that can say anything they like, true or misleading. Thirdly, there are now such enormous volumes of valuable data on the internet that anyone with criminal intent and technical expertise can seize that data and misuse it, causing enormous damage and loss to others in the process.

As a result, crime prevention work now extends to areas such as **phishing**, **hacking**, **scams**, **cyber bullying** and **sextortion**,

specifically. This booklet thus pays particular attention to these fields. And then there is the gigantic minefield of **internet pornography**, which is dangerous to children, young people and adults in equal measure. The fact that legislators' proposed protections for children and young people in this area are practically ineffectual is a sad reflection of society vs. technology – evidence that, to some extent, society itself has become a victim of the rapid pace of its own technological development.

Alongside these new dangers in the digital world there are still the "conventional" forms of crime: fraud and theft, burglary and robbery, domestic abuse and violent public order offences, vandalism, bullying, mobbing and stalking, threatening behaviour and extortion, sexual assault, abuse and rape. The list is long, and it is difficult to classify these offences effectively into groups such as violent crime, sexual offences and property crime. The characteristics of different types of offence often overlap. For example, should a mugging be classified more as a "violent crime", or as a "property crime"? Is sextortion – online extortion using videos of a sexual nature which the victim did not wish to record – a sexual offence, classic extortion, or a form of internet fraud?

This security guide will avoid becoming too technical, and the recommendations it contains will not go into excessive detail about specific threat scenarios. Comprehensive information and tips on how to behave in the situations mentioned are always available on the www.skppsc.ch website (in German, French and Italian), or in one of the advice leaflets issued by SKPPSC Swiss Crime Prevention. The chief aim of this brochure is to provide information about the considerable

breadth of problem areas in which crime is now commonly being committed – and in which crime prevention work is both possible and useful.

When you have finished reading, you may feel uneasy about the immense criminal energy, creativity and ruthlessness which people apply to harming others and thereby gaining benefits for themselves. Equally, you may perhaps feel better prepared, because you are no longer as trusting, unsuspecting or credulous as you might have been, and are more critical, alert and well informed. You may also have been confirmed in your belief that, despite everything, it is worth standing up for fairness and justice, on the internet just as in real life. We should also not forget that Switzerland is one of the safest countries in the world, in which each of us can protect ourselves effectively against crime by conducting ourselves correctly. It is also a country in which the victims of crime are supported.

The Police Forces of Switzerland



1. Violent crime

Many cases of violent crime are not about any advantage for the perpetrator, but about causing harm or distress to the victim: they attempt either to damage the victim mentally, with psychological weapons, as is the case with bullying, mobbing and stalking, or to physically attack them. Threatening behaviour (which also forms part of the pattern of harassment, bullying and stalking) is a hybrid form of these offences, because the prospect of severe, and often physical harm, affects the mental health of the victim. In some cases, the victim may simply be a passer-by, as is the case with violent public order offences, or they may be affected indirectly, for example by vandalism, i.e. damage to property. Equally, vandalism may be targeted, if the destruction of physical property is intended to harm a specific individual, group of people, or even "the state". Finally, in the case of domestic abuse there may be a fluid mix of mental and physical forms of abuse. As mentioned above, it is difficult to classify the various forms of offence conclusively.



Domestic abuse begins with the **minimisation** of the victim. For example, where a husband dictates his wife's every move, where he alone makes all the decisions including what she is "allowed" to do or "forbidden" from doing. It is all-pervasive and accompanied by the threat of punishment: that is domestic abuse. In our society, enormous importance is attached to **self-determination**, and anyone who attempts within an intimate relationship to limit another person's power of self-determination and freedom of action by means of threatened or actual **abuse** – be it **physical**, **psychological**, **sexual**, **financial** or **social** in nature – is punishable under the law. In this context, the intimate relationship may be a marriage, a marriage-like relationship or a relationship within a family. It might be a current relationship or one which has already ended.

Social abuse describes situations in which the victim's social contact is determined by another person, for example where a husband takes his wife's house keys away and forbids her to meet with the neighbour. Financial abuse covers being both forbidden from working and forced to work, the confiscation of wages, as well as situations in the partner has sole powers of disposal over financial resources. Sexual abuse includes forced sexual acts up to and including rape, while psychological abuse covers intimidation, threatening behaviour and coercion. Finally,

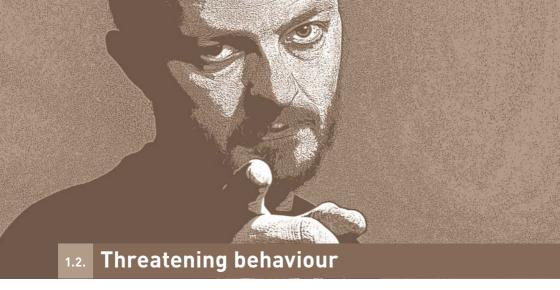
physical abuse may begin with a **slap**, progress to **persistent beating** and, in extreme cases, end in **murder**. These forms of abuse are rarely found in isolation, and often overlap.

The list of possible victims of domestic abuse is thus correspondingly long: women, men and young people in both straight and gay relationships, children who are abused by their parents, parents who are abused by their children, grandparents who are mistreated or – if in need of care, neglected – by their children, young women forced into marriage, young victims of female genital mutilation, victims of "honour killings", etc.

What you should do:

Every individual who is confronted with some form of domestic abuse should be very clear about one thing: domestic abuse is not a private matter. Most domestic offences are statutory offences. In other words, in their capacity as a law enforcement authority the police are required to investigate. Unlike victims of other statutory offences, those affected by domestic abuse have certain options to have those investigations suspended. These are limited, however.

As a result, the police only need to be aware that the abuse is happening to be able to intervene immediately. This places an obligation on everyone who knows of or suspects domestic abuse, although they may not be affected personally: neighbours, friends, relatives, colleagues, etc. If you suspect that domestic abuse is taking place, and of course especially in urgent, violent situations – for example, if you hear a loud argument and the sound of someone being beaten in a neighbouring flat, or if you hear cries of pain or for help, please immediately call the emergency police number, 117. There are a whole range of support and counselling services available for both (potential) victims and (potential) abusers. These should be contacted at an early stage, but are also on hand when the abuse or violence has already escalated.



Threatening behaviour is advance warning of action that will harm the subject of the threat. However, for such behaviour to be prosecuted as a "serious threat", it must be credible, its content must be to the considerable detriment of the victim, and it must cause genuine fear and alarm to the victim. Whether or not threatening behaviour is prosecuted is thus ultimately determined by whether or not the person being threatened actually feels under threat and reports the behaviour – and not by whether or not the threat really was meant seriously, in other words would it, in the event of doubt, ever be carried out? The form of the threatening behaviour – verbal, written, by email or anonymously via a social network – does not matter.

In most cases the context, involving the friends, family and previous history of those concerned, will permit a realistic (to some degree) assessment of the actual severity of the threatening behaviour, although of course misjudgements can happen. For example, to give an extreme case, where someone wishing to leave a criminal association is threatened with death, there is good reason to take that threat seriously if other who have previously left have actually been killed.

What you should do:

If someone threatens you, and you feel genuinely at risk as a result, please notify the police so that they can assess the situation with you, identify the person behind the threat, interview them, and prosecute them if appropriate.



Violent altercations mostly involve young people, at sporting events or demonstrations for example, and **alcohol and drugs are often a factor.** In such incidents, aggressive groups of people clash with other aggressive groups – or with the police who are preparing to deal with such clashes. In rarer cases, the aggression is directed towards random passers-by or towards individuals who, seeking bravely to intervene in the conflict, have further inflamed it.

What you should do:

To minimise the danger of an attack on your person, avoid places in which violence tends to breed, such as the areas around railway stations at night. If you are approached aggressively, try first of all to get out of the situation by walking away calmly, standing tall. If someone blocks your path, try to stay calm and focus on communicating with one person in the group. This is the time to maintain eye contact to show that you are not afraid – even if that is not the case. If you are attacked physically, try to run away, shout for help, and defend yourself as best you can. If you witness a violent altercation, intervene only if you are certain that you can help the victim. Mobilise other passers-by, but do not put yourself in danger. It is better to wait at a safe distance to help the victim once the attackers have gone. and to watch events closely so that you can make a useful witness statement later on. Whatever happens, always call the police.

1.4. Vandalism

Vandalism is not a criminal offence in *itself*, but as "unlawful and deliberate damage, defacement or destruction of items of public or private property" it almost always qualifies as the offence of criminal damage. The actions of vandals, who are almost always young people, are sometimes described as "blind destructiveness", but in most cases they know precisely what they are doing when they scratch cars, spray graffiti, smash windows, lay waste to parks, remove manhole covers or put lit fireworks in letter-boxes. In doing so, they know full well that not only are they destroying property, but that, because of their destructive act, people will also face injury or financial loss, for example that someone may fall into an open manhole. In such cases, criminal damage is accompanied by much more serious offences.

What you should do:

For the reasons described above, it is important that witnesses to vandalism report it to the police. If you see that someone is damaging someone else's property, watch closely and then report it on the **emergency police number, 117.** Do not intervene yourself, however, as there is always the risk that the vandal will turn their aggression against you, and that criminal damage then becomes assault, especially since alcohol is often involved and inhibitions are already lowered.



Bullying is a relatively widespread phenomenon in our society. and the technical opportunities that the internet offers for cyber bullying has lent it even more potential to do harm. A group deliberately inflicting psychological injury on an individual in order to **isolate** and **exclude** them is referred to as mobbing, which is a particular form of bullying. While workplace mobbing is primarily a means of encouraging unpopular colleagues to leave, mobbing at school, in sport and on the internet is often an end in itself. In other words, the target need not even be particularly unpleasant. In many cases, a minor incident, or a moment of weakness or embarrassment is all it takes for a mobbing community to form very quickly indeed. These bullies bully simply because they can. They do so by insulting, mocking, harassing and defaming their victims, and may even go as far as coercion, threatening behaviour, extortion and physical **assault.** In the case of cyber bullying, this primarily takes the form of malicious posts and comments on social media, where physical assault may also rear its head in the form of video clips.

Bullying almost always begins in real life, and although cyber bullies like to conceal their identity, the victim and bully will generally know each other **personally.** Bullying *in itself* is not defined as a criminal offence, but many of the methods mentioned above may constitute and be prosecuted as **serious offences.** Indeed, extortion and coercion are statutory offences – something often forgotten by cyber bullies who feel safe hiding behind their (supposed) **anonymity** on the internet.

The causes and consequences of (cyber) bullying cannot be generalised, but there are naturally common threads: power plays, **group dynamics**, weak or inflated egos, instigators and followers, and the **lack of empathy** on the part of the perpetrators. Although it is sometimes possible to reconcile the bully/bullies and their victims, an additional problem with cyber bullying is that, **once online**, all **defamatory**, **libellous and untruthful posts can still be reposted unchecked!**

What you should do:

If you yourself are being bullied or mobbed, try above all to stay calm and composed. Collect as much evidence as you can: save chats, e-mails and user names, and take screen shots. You should also notify the police, which will review the **relevance** of the material under criminal law so that, if appropriate, you can make a formal complaint. Alternatively, if it is clear that a statutory offence has been committed, the police can begin investigations directly.

If someone you know is being bullied or mobbed and is distressed as a result, let them know what legal options are open to them. If your child is being bullied, your first course of action is to try to speak to teachers and parents. If that does not resolve the situation, then contact the police. Nobody has to accept mobbing, bullying or cyber bullying. In your personal dealings with others, and online, watch that you do not get carried away being insulting or hurtful, even if the other person does. Refuse to sink to their level, as doing so may put yourself in legal jeopardy.



Stalking describes the intentional, repeated pursuit and harassment of a person that may threaten or damage their psychological and physical integrity. There are a whole variety of reasons for someone to pursue and harass another person. For example, it may be a rejected former partner who cannot cope with the end of the relationship and becomes fixated on the idea that it can be revived with flowers, gifts, daily emails and telephone calls at all times of the day and night (telephone harassment). Or it might be the fan of a famous pop star, who **obsessively** pursues their idol's every step, stays in the same hotels and is standing at their garden fence whenever they look out of the window, convinced that they and the star belong together. Someone might also become a stalker out of a desire for revenge, for example if they hold a specific person responsible for some negative event in their life, and thus attempts to bombard them with acts of **psychological terror.** They might post a fake death notice or advertisement for sexual services, or create fake social media profiles which they then use to cause maximum damage to the victim's reputation. They might even break in to the victim's home in order to leave signs of their presence or to take specific items.

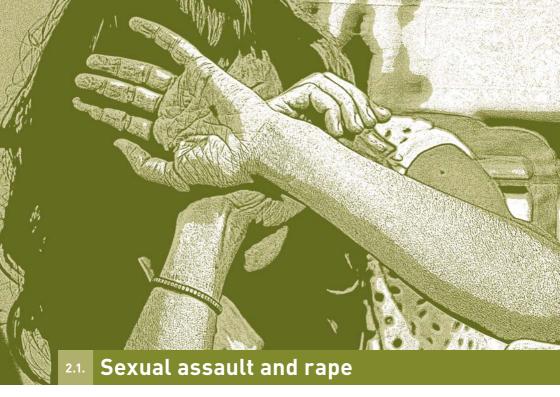
Although mobbing, bullying and stalking do not constitute independent criminal offences in Switzerland, the law in almost every canton makes it possible for stalkers to be approached as potentially threatening individuals, for them to be detained temporarily depending on the outcome of a risk analysis, and for them to be placed under a fixed-term restraining order forbidding contact with the victim and any children, and instructing them to stay a certain distance away. Where necessary, there may be the threat of consequences under criminal law if the order is violated.

What you should do:

In the interests of efficient crime prevention, it is important that you recognise at an early stage that you are being stalked, and that you take appropriate action. The first step is to speak directly to the stalker - providing, of course, that you know them - and to make it unmistakeably clear that you do not wish to have any (further) contact whatsoever with them. You can also write to them, formally excluding them from your property. If it is not possible to resolve the situation by speaking to the stalker, or if the stalking continues regardless, tell your friends and family what is going on, to avoid any misunderstandings. You should also collect as much evidence of the stalking as possible. Notify the police so that they can assess your level of risk, and make a formal complaint if appropriate. Although the stalking in itself may not be an offence, the stalker's individual actions. such as threatening behaviour, coercion, trespass, defamation, and even the rather oldfashioned-sounding "misuse of a telecommunications system" are punishable under the law.



2. Sexual offences



Sex is part of life and can be practised in countless different ways – providing it is **consensual**, between adults or those who are above the **age of consent**.

However, anyone who forces someone else to have sex, or uses violence to bring about a sexual act, is punishable by law, regardless of whether they are motivated primarily by sexual satisfaction or by using sex as an **instrument of power** to degrade another person and make them submissive. It may be a husband who rapes his wife, a boss who coerces his secretary, or a photographer "casting" a model. Whenever sex is non-consensual, someone is committing a criminal offence.

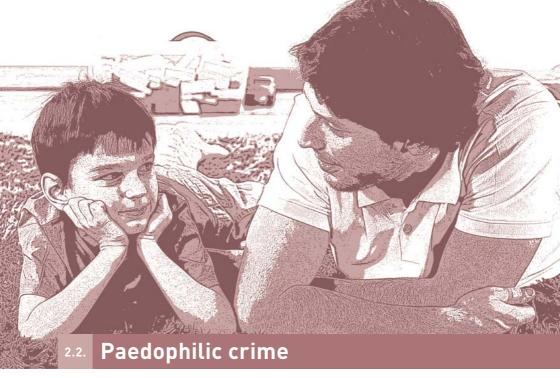
That sounds very clear-cut, but in reality it is not. In fact, experience has shown that it is often very difficult to prove violence and force where sexual acts have already taken place, and the other side claims that they were consensual. It is equally difficult to prove consent if this is subsequently disputed by one of the parties. The police must investigate as soon as they become aware of any allegation of **sexual acts involving children, dependants,**

or those incapable of judgement or resistance, sexual coercion or rape, because these are statutory offences.

Even the attempt to bring about sexual contact (whether serious or apparent), such as suggestive remarks, gestures or unwanted touching, can be classified as **sexual harassment**, and thus constitute a criminal offence. Sexual harassment is an *offence prosecuted on complaint*, however. In other words, anyone who feels harassed must make a formal complaint if they would like the police to investigate.

What you should do:

It is up to you to decide whether or not you would still let something pass as clumsy flirting if your sister or work colleague, for example, would very definitely classify it as sexual harassment. As soon as a situation involves sexual acts that you in no way want, defend yourself and call the emergency police number, 117. You should be particularly careful if the parties have been drinking alcohol, because it lowers both the inhibitions of the potential perpetrator and the resistance of the potential victim. In bars and at parties, make sure that nobody spikes your drink (keep it in sight or finish it, but never leave it sitting half-full). If someone attacks you physically, use all that you have to defend yourself - scream and fight back. That is enough to put many attackers off. If the attack does result in rape, seek medical help immediately so that the evidence can be secured. Victim support services can advise you, and you can also decide at a later point in time whether or not you want to submit a formal complaint.



The **age of consent is 16** in Switzerland. Under this age limit, sexual acts are punishable offences unless the age difference between the parties is a maximum of three years – and the acts are consensual. However, if the age difference is greater, they are classified as **sexual acts with children**, i.e. a **paedophilic offence**, which covers not only rape, but also in appropriate touching and French-kissing.

Two facts are worth noting here. The first is that, in the great majority of cases of child abuse, the perpetrator (usually a man) is someone from the victim's **close circle**, in other words their family, school, sports club, church, or a music teacher. The victim knows the perpetrator, was entrusted to his care, and trusts him. Although it is still generally assumed that the proverbial "dirty old man" is a nameless monster, he is much more often genuinely an older man that the child knows – although of course that does not in any way mean that all older men are "dirty".

The second is that **paedophilic crime** and **paedophilia** are not the same thing. Paedophilia is the diagnosis of a sexual orientation which simply indicates that the paedophile feels sexually attracted only to children – which has no consequences under criminal law as long as such feelings are not acted upon. By contrast, the committer of a paedophilic crime does not have to have paedophilic inclinations to sexually abuse children. Often, they genuinely do not. Their motives might be, for example, perverted curiosity, sadism, or fantasies of power. Consequently, paedophilia in itself is not necessarily condemnable, but requires medical treatment, because it can lead to paedophilic crime, which is without exception a criminal offence.

What you should do:

To prevent potential abuse, it is first and foremost essential that vour child trusts vou and that vou trust your child! For decades, children's attempts to tell their parents of abuse fell on deaf ears, or they were told off for "lying" and even punished. Abuse lay outside the realm of what parents could imagine happening to their children. Today, there is an awareness that child abuse can happen even in settings that are thought to be safe. You should therefore be aware of this fact, and should also take every opportunity to explain the facts of life to your child in an age-appropriate way. Bring them up to be a self-confident individual who knows how to set boundaries. Of course, vigilant adults will keep an eye not only on their own children, but also on those around them.



2.3. Illegal pornography and sexting

In view of the vast volume of pornography that is now available, especially on the internet, you might think that the technical developments achieved by all humanity have always been working towards a single, covert objective: to send and receive porn. From our crime prevention perspective, porn is important only with regard to the following aspects: **the law forbids making pornography available to anyone under the age of 16.** That means that the 12-year-old who can access the most extreme hard-core porn film with two mouse clicks is not at fault. The fault lies with the countless providers with countless servers in countless locations both in Switzerland and abroad. Clearly, however, that also means that the law cannot be enforced. And it also means, of course, that no way has yet been found to prevent almost any child under 16 coming into contact with pornography nowadays. The effects of this remain to be seen.

That said, we are talking here about **legal pornography**, which is not regulated *in itself*, but only in relation to its consumption. Also available – albeit requiring more than a couple of mouse clicks – is **illegal pornography**, which by contrast is *prohibited in itself*. It is classified as **pornography involving animals**, **violence**, **and children (or minors)**, and is illegal because it constitutes the **documentation of a criminal act**. Behind every child porn film is a real child who is genuinely being abused in some form or other. It might therefore be said that anyone consuming this type of pornography is indirectly supporting the sexual exploitation of children. Any contact with illegal pornography is

therefore a statutory offence. Young people who (inadvertently) become providers of pornography constitute a special case, however.

Nowadays, when teenagers fall in love it often doesn't take long before they are taking nude photos of themselves with their smartphones, or filming sexual acts, and sending them to each other. It is referred to as "sexting". However, what teenagers generally do not realise is, firstly, that no photo that is released into the digital world can ever be retrieved. It is always possible that someone, somewhere, will distribute it further or use it specifically as a means of bullying. Secondly, depending on their age, they may be skating on the thin ice of illegal pornography. For example, if a 15-year-old takes pictures of herself naked, in a sexy pose, and sends those pictures to someone else, from the legal perspective she is regarded as the producer and provider of child pornography. However, to avoid turning sexting teenagers into criminals unnecessarily, teenagers between the ages of 16 and 18 are exempt from prosecution if they only share their photos between themselves, and do not send them on to any third party.

What you should do:

Talk to your children about the problem of pornography and illegal pornography, especially child pornography and sexting. If you should come into contact with illegal pornography in any form, whether on the internet or among your friends and relatives, it is best to involve the police immediately. Do not be tempted to "secure evidence", however, as you yourself will be liable to prosecution if you are in possession of illegal pornography. If you feel sexually attracted to children, speak to a doctor you trust, or get in touch with one of the addresses listed for this issue on the SKPPSC Swiss Crime Prevention website.







In the legal jargon, fraud is defined as the intent unlawfully to enrich oneself or another person by misrepresenting or concealing facts to maliciously deceive someone or to maliciously reinforce a misconception, and thus force the person holding that misconception into behaviour that causes a financial loss to themselves or to another person. As mentioned in the introduction, the internet is a particularly effective vehicle by which to misrepresent and conceal facts because, initially, nothing can be proven. Everything is virtual, rather than being physically present. The internet thus provides the perfect marketplace for offers that, in reality, do not exist, offered by people who prefer to remain anonymous. This has allowed a particular form of fraud to become established: the scam, which appears in countless, ever-evolving forms.

The principle is always the same: in a scam, providers promise products, services or even high sums of money that can be obtained only against a certain advance payment. If the offer were genuine, the advance would be extremely small in comparison to the promised value of the offer. That is what makes it so attractive. However, regardless of whether the advance is high or low in absolute or relative terms, it is lost in any case, because no product or service will ever be provided in return.

New online shops are opening up every day as part of the global trend of retailing increasingly shifting on to the internet. Some of these are set up solely for fraudulent purposes and are not, in fact, proper online shops at all. They simply appear to be. Instead, they are **fakes.** In many cases, the products they offer are the same as those sold by competing providers, but the prices are unbeatably low. However, anyone ordering from these "shops" and transferring money in advance will receive substandard goods, if anything at all.

What you should do:

Fake online shops generally look very professional, so that it is impossible at first glance to tell them apart from genuine retailers. However, if you can avoid being taken in by their cheap offers, you're likely to find countless spelling mistakes, which are rarely found on the sites of bone fide retailers, and are a major clue that the provider is a fake. There are also quality marks that you can check, such as the "Swiss Online Guarantee" issued by the Swiss association of mail-order businesses, VSV, or the "Trusted Shops" mark. Check both portals to ensure that the mark really has been awarded to the site you're looking at. As a general rule, it's worth checking all of the potential weak points of any online shop: how do the payment and delivery terms look, and what about the publication details (if there are any at all!)? Does anyone answer the customer service number, or mails that you send? Where is the company based? Are there any customer ratings (and are they credible)? And so on. The fewer details you can find about the identity of the provider, the greater the probability that the shop is untrustworthy.

In the case of a **car scam**, you buy a car cheaply via the internet, and are promised that it will be delivered to you at home very soon. While you happily believe that it is already on its way, and look forward to taking possession, you hear from the supposed transport company, demanding an advance payment to deliver the car or, depending on the agreement, the full price. You pay the money but get nothing, because in reality the car was not for sale at all, the transport company doesn't exist, and the seller is a fraudster.

Property scams work in a very similar way, but instead concern flats and houses offered for rent via the internet. A well-appointed flat in a great location, which is relatively affordable and hasn't yet been snapped up is a dream for many home-hunters. So you send an email saying that you're very interested, and remarkably quickly you are told it's yours, providing you transfer a "deposit" to the supposed landlord before you get the keys or can even view the property. You subsequently find, however, there is neither a key nor a viewing, because there was neither landlord nor flat!

The financial loss can be even greater where this sort of scam is used to offer a **holiday home**, especially in high season when everything else is already booked. In such cases, you not only lose your deposit, but have ultimately also paid to get to your holiday destination, may possibly have to stay somewhere expensive, organise your return journey, and finally get over the fact that you have been robbed of your relaxing holiday!



The **lottery scam** has become something of a classic in its genre: you get an email, text message or letter notifying you that you have won a foreign lottery. The amount involved is generally in the millions and, in comparison, the sum that you are being asked to pay in advance to cover the money transfer and "general administrative costs" seems negligible – although it can quickly add up to thousands. You're happy to pay, but get nothing, and also never hear from the lottery again. Only too late do you realise that, to win a lottery, you first have to buy a ticket...

A particularly devious – but also transparent – form of scam is the **emergency email** that a fraudster sends to you in the name of someone you know. They will previously have hacked into this person's email account (see sections 3.2 and 3.3 on phishing and hacking), and is now going through their address book. They then send a heart-breaking mail to everyone on the list, telling the tragic story of how they (i.e. the person you and everyone else knows) have been robbed, are stuck at some foreign airport without any money, and desperately need you to make an immediate cash transfer so they can buy a ticket to fly home.

More underhand still is the **love scam** or **romance scam**, as in addition to causing financial loss, it also leaves broken hearts in its wake. People looking for a romantic partner (in many cases women) go on internet dating sites and social media, where they are initially showered with compliments and declarations of love by foreign fraudsters assuming false identities. Having convinced their victim that they are in the happy yet confusing throws of love, the fraudster moves in and asks for money – for a flight ticket, a visa and a passport to finally make that longed-for first meeting happen, for example. Alternatively, they may tell their victim that they need to go into hospital, or that there is some other family emergency in their home country. Victims often hand over everything they have, and only then do the fraudsters abandon them and turn their attentions to their next victim.

What you should do:

There are always three things that you should be aware of with offers and claims on the internet. The first is that **if an offer seems too good to be true, then that's exactly what it is – too good to be true!** Only in fairy tales do two people fall madly in love with each other without ever having met. There is no latest-model car, in mint condition, at half list price. If every flat viewing in your city attracts a long queue of potential tenants, why should you, precisely, be accepted by email that very same day? Sea view, fully equipped, twenty metres from the beach, high season, affordable and still free, one day before you fly? Impossible. Lotteries

without tickets, inheritances without relatives, Canadian engineers who want to share their life with you? There's no such thing.

The second is that you should always check the identity of the person making the offer or request, but disclose as little data as possible yourself. Never send out copies of official documents, because they could be used for forgeries. If a friend or acquaintance asks you for help by email, first try to reach them by phone or in person to find out exactly what is wrong. You will probably notice simply by the style in which the mail is written that something doesn't add up. What's more, you probably aren't the first person that your acquaintance would ask for money in an emergency, so why you, now?

Thirdly, opt for secure payment methods! Be vigilant if you are asked to make an advance payment using a money transfer service (such as Western Union or Moneygram) or to an account abroad (such as in Spain, the UK or the Middle East), whatever the reason, even if it is apparently to your advantage. Flows of funds cannot be traced via money transfer services, and the Swiss prosecuting authorities will often have only limited access to foreign accounts – ideal for fraudsters!



Phishing is an invented, hacking-related term which refers to "fishing" for passwords and other confidential data. It describes a form of data theft via the internet, aimed at facilitating property crime. This is how it works: the fraudster sends you an email or a message to your smartphone, claiming to be a reputable institution (such as your main bank, the post office, an online auction house or an authority) which requires your active support with an urgent problem, such as closing a security loophole. You are then referred to a certain, entirely genuine-looking website, where you are asked to enter your personal access data, passwords, transaction numbers (TANs) etc. - which you do willingly, because problems need to be solved! In reality, however, the website is fake and you have just handed control over your bank account, or some other account, to persons unknown. The fraudsters will then raid your account in your name, make purchases, continue to send out fraudulent messages, or even offer goods for sale in your name that will be ordered and paid for by the next victim, but never delivered.

What you should do:

Assume that anyone claiming that they can only solve some form of problem if they have your passwords is a fraudster. No bank and no reputable company will ever ask you to enter your personal data anywhere, unless the contact is instigated by you. Therefore, if you get a message like that described above, don't respond to it and don't click on any links! However, if you're not sure whether or not you have already fallen victim to phishing, immediately contact your service provider and describe what has happened. They will be able to help you. You can also report the attack to www.antiphishing.ch.



In computer jargon, **hacking** refers to overcoming security features to penetrate a foreign computer system with viruses, worms and trojans, for example. The target might be a website, an email account, or simply your laptop on your desk. The aim of the attack is to modify the content and structures of the foreign system as the hacker wishes. To do this, the hacker installs **malware**, which gives them complete control of the target system.

But why? The motives can vary widely. Perhaps the hacker is looking for data which is useful to themselves or to their client, but which cannot be obtained by legal means, or perhaps they want to delete certain data. They may wish to disrupt others' business relationships, block ongoing deals, or gain control of sensitive technical equipment in order to extort someone. Or they may hack simply because they can. In any event, **extortion** is a common motive for hacking, in which the hacker generally promises the victim that they will de-install the malware, i.e. release the victim's system, in return for a certain sum of money.

What you should do:

As is so often the case, there is no 100% secure way to protect yourself against being hacked, because technical developments will keep creating new security loopholes through which viruses, worms and trojans can infiltrate foreign systems. You can nonetheless minimise your vulnerability by choosing a secure password and by installing anti-virus software and firewalls. Please ask your retailer or service provider which products are most suitable for your system. Furthermore, you should be basically sceptical if you are contacted by unknown providers by (spam) email or when surfing on the internet - open mails and attachments only if you know the sender, and don't download any programs from unverified sources. In addition, do regular backups so that you're not completely dependent on just one hard drive. If you have been hacked and are being extorted, immediately contact the police.



Sextortion – describing extortion through sex – has become a common online offence which functions as follows: the target, who is usually a man, is contact via a dating platform or social media by an attractive woman who claims to be very sexually open. After the initial flirting, she recommends switching to a video chat to get to know each other better. Given the "electric" atmosphere between the two, she suggests that they both should undress and masturbate directly in front of the camera. To prove that she is serious, she immediately begins, to which the man responds – perhaps after a moment of disbelief – by also undressing and masturbating. What he does not know, however, is that everything he does in front of the camera during the video chat is being recorded.

Some time later the woman contacts him again and demands that he pays her money otherwise, she threatens, the video showing his "performance" will be published on the internet and also – depending on what other data the man has disclosed about himself – sent to family, friends or his employer. In another form of sextortion, which arises out of sexting, for example (section 2.2), a private sex film (recorded initially in full intimacy and trust) is used to force the victim – in this case generally female – not to pay money, but to engage in further sexual acts.

In this case, this section would be better titled "what you shouldn't do"! If you don't exactly have exhibitionist tendencies and thus don't consciously take the associated risks, do not engage in any sexual act in front of a camera. In most cases, where there is a camera there will be a storage medium nearby, and once something has been stored, it may fall into the wrong hands. If you have already been caught in the sextortion trap, on no account give in to demands for money, because it in no way quarantees that the material will not be published, and may be followed by further demands. Instead, notify the police and make a formal complaint. Even though the whole incident may, understandably, be embarrassing for you, remember that the police investigate crime, not human weakness!







Theft is probably the oldest and most common offence of them all, in which the perpetrator appropriates moveable property belonging to someone else with the intention of unlawfully enriching themselves or others. Thefts primarily concern money, bank cards and jewellery, smartphones and laptops, bicycles and cars and, less commonly, livestock, outboard motors and construction cranes...

Sneak thieves enter unlocked spaces, for example in sprawling, anonymous office complexes, or retirement and care homes, and also like to sneak into houses during the day through an open terrace door. Pickpockets seek out crowds at concerts, sporting events, demonstrations and public festivals, on escalators and in public transport; confidence tricksters distract their victims, in public by jostling them or asking for directions, and at the door, by faking an emergency, or claiming to be a tradesperson who needs access to do the job they have been asked to do. Pickpockets and confidence tricksters often work in teams of two or three. While the first person distracts the victim, the second steals their wallet and passes it on to the third, who disappears into the crowd. At the door, the first thief engages the victim in conversation while their partner slips inside and combs through the house or flat.

In this way, many thefts occur as a result of the **victim's care-lessness** – by not locking doors, not watching bags, not securing bikes, and being too trusting in letting a thief into their home. It's a clear case for crime prevention!

What you should do:

When you leave the house, take only the cash and valuables that you actually need. Carry them or your handbag close to your body, and put your smartphone and wallet in inside pockets. Never put valuables down anywhere, even for a short time, such as your phone on a cafe table to open the zip of your bag, or your wallet on the counter while you insert your credit card in to the terminal, or your wedding ring on a public washbasin when you go to wash your hands. Many thieves specialise in these brief moments of opportunity. Keep everything in your hand and in sight.

When you travel, watch your luggage, and never deposit it anywhere out of sight. Also remember that your bag can be **snatched** with force, for example by a thief riding by on a moped. This is a common form of theft at many tourist destinations.

To secure your **bicycle** or **motorbike**, whenever possible lock it in a secure space, otherwise use a **verified security lock** to attach it to a **firmly fixed object**. For your car, choose well-lit, open car parks and parking spaces, lock it properly, and keep your car key safe so that it can't fall into the wrong hands. What's more, don't leave any valuable in your car, whether **visible or in the boot**.

If an unexpected stranger rings your doorbell, don't simply let them in. Anyone claiming to be a tradesperson or official should show you their ID through the spyhole, and state which company or authority has sent them. Don't ask for a phone number, however, as it might be fake. Instead, regardless of how long it takes, find the company or authority's contact details out yourself via the internet or in the phone book, call them, and ask them to confirm that they have sent the person in question.



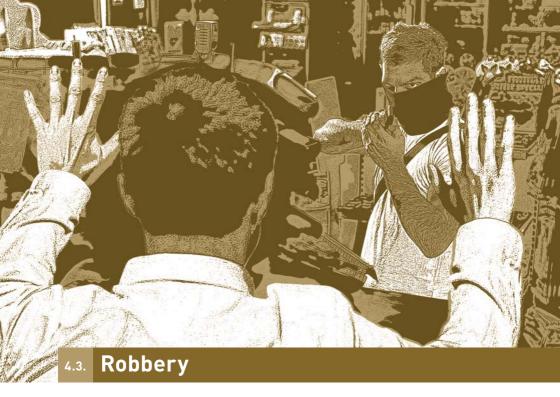
A thief who has to break open a door or smash a window to enter someone else's property is referred to as a burglar. However, if the door is left ajar, or the window is open, the thief is able to **sneak in** (see previous section), which can make a difference to the victim especially where insurance is concerned. Remember that windows that are tilted open still count as being open. The majority of break-ins in private houses and flats happen during the day, because it is then that most people are at work, running errands, or have appointments elsewhere. Conversely, burglars prefer the **night** to target offices, business premises and warehouses, because the working population is then back at home. Most burglaries happen quickly and inconspicuously, without any special tools. In most cases, simple crowbars and screwdrivers are all it takes to lever open doors and windows which do not have any additional security. That said, burglars do not particularly like taking risks, and will give up quickly if they meet greater resistance. That is where you have the chance to protect yourself effectively.

Always close all doors and windows when you leave the house, even if you're only going to be away for a short time. If you're away for longer, especially during the winter months, consider having lights on a **timer switch**, to make it look like you're home.

You can also have a security expert from your local police force advise you on structural and mechanical security measures, such as additional locks, bolts and window grills, as well as on electronic security systems such as motion sensors with floodlights, and alarm systems.

It is also very important to have a **good relationship with your neighbours**, who can keep an eye on your home especially when you are away on holiday, and can empty the letterbox so that it doesn't overflow.

Should you catch a burglar red-handed, don't try to detain or overpower them. Instead withdraw, lock yourself in at home, and call the **emergency police number, 117.** If you can, observe and note down everything connected with the break-in, such as the burglar's appearance, the number plate of their getaway car, etc.



Robbery might be described as an aggravated form of burglary, because in this case the violence is directed not (only) against doors and windows, but against people. Thus, robbery is always classified as a violent crime. However, the actual motivation for a robbery is always the prospect of making a gain from someone else's property. The primary targets are banks, foreign exchange bureaux and money courier services, (luxury) shops, travel agents, kiosks and filling stations, as well as, less commonly, private individuals, either at home or in a public place. These robberies are usually planned very carefully, with the robbers expecting to come away with a specific haul. They threaten their victims with physical violence or with firearms, and may even carry out those threats to force the handover of money and other valuables. If you are the victim of a robbery, you are in **considerable danger**, and should therefore try to act very calmly.

In the event of a robbery, keep calm. A robbery is an extreme situation for the robbers themselves, as well as their victims, and they may tend to over-react. As far as is possible, you should therefore do what they ask, don't provoke them verbally, and do not make any sudden movements or scream loudly. Do what the robbers tell you to do, because you might genuinely be in a life-or-death situation. When the robbery is over, immediately call the police, help others who have been affected, and please make yourself available as a witness.



The tricks that fraudsters use on the internet to try to part you from your money are covered by section 3 of this booklet. We will now turn our attention to forms of fraud which do not need the internet at all. Instead, they are perpetrated via the good old **telephone**, or by a personal approach at the **door**.

We are all familiar by now with **fraudsters posing as long-lost relatives** – but that doesn't mean that the scheme no longer works. The perpetrator telephones an elderly person claiming to be a young relative who is having an emergency, and therefore needs money. They say that they are unable to go round to collect the money themselves, so will have to send a friend. The trick here is for the person the elderly relative *thinks* is calling to be distant enough that their voice doesn't give the game away, but not so distant that the elderly relative wouldn't immediately offer financial help if they needed it. But who might it be? The elderly person knows best, thinks the fraudster, and so asks them: "guess who?", which gets the elderly person thinking about a **trusted person who lives far away**, perhaps a family member, or some old friend. The fraudster on the telephone is only too happy to take on that role and play it to the hilt.

In a particularly despicable form of this **telephone fraud**, the "guess who?" call will be followed soon afterwards by a call from a second fraudster, who claims to be a police officer

investigating confidence tricksters, and offers their help. For an elderly person who thought perhaps something wasn't quite right, they can seem like a saviour. A short time later, the fake police officer is at the door, offering to take cash and jewellery and put them "in a safe place"... In some cases, the fake police officer will call "spontaneously" to warn the elderly person that there has been a series of break-ins in their area, and tell them that they will call round to take valuables away for safekeeping. Regardless of the current form that this fraud takes, the ultimate objective is for the victim to hand over cash and valuables to a stranger who is either in uniform or claiming to represent someone the victim knows.

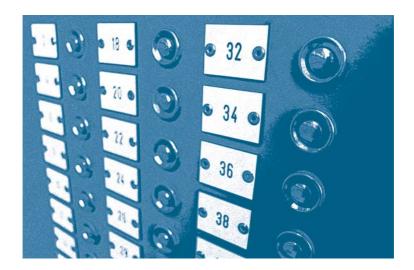
What you should do:

If someone calls you and asks you to guess who they are, and you do not recognise their voice, insist that they tell you their name and then **check that they are who they say they are** by asking questions such as "what's my sister's name?", "where did I last go on holiday?", or "when is my birthday?". If the caller can't answer, or becomes aggressive, they clearly don't know you, so simply hang up the phone.

In the case of callers who say that they are a police officer, IT support or any other service provider, and ask you for personal data, financial information or passwords, you are most likely dealing with a fraudster, because **no reputable institution will ask you to disclose personal or even secret data over the phone.** If you aren't sure, speak to someone you trust. What's more, no police officer will ever ring you from the 117 emergency number. If this number appears on your display, it has been **manipulated to trick you (known as spoofing).**

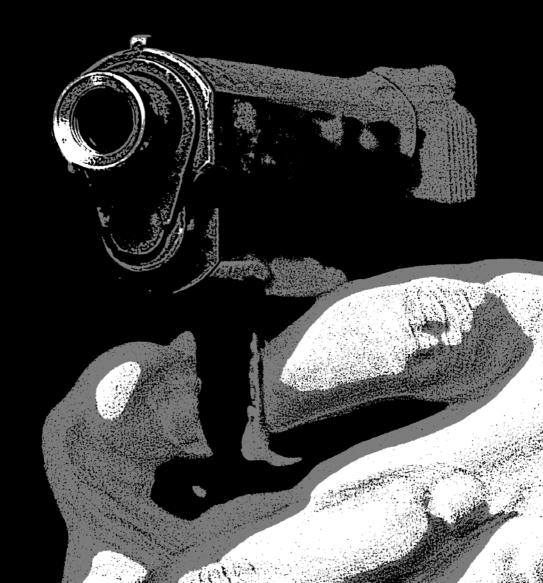
Do not tell or show anyone where you keep your cash and valuables, and never hand over money or valuables to people you don't know, even if they claim to be representing a relative or friend.

Where door-to-door salespeople are concerned, be vigilant if you notice anything resembling this pattern: the salesperson at the door immediately pushes their way into your home, because they don't want your neighbours to see or hear them as they draw you in with their spiel. They would much rather do that sitting on your sofa in your living room. The salesperson will present you with unbelievable special offers, such as a topquality set of knives from Solingen, a beautiful Nappa leather jacket, or a genuine Persian carpet - and all at a fraction of the horrendous original cost, as shown on some price tag that they show you as evidence of the item's value. They may even have **branded goods** with them, such as personal care or household items. In any event, they will insist that they only offer the very best products at the very lowest prices - and will insist on cash payment. In return, you will receive a proper receipt showing the letterhead of the fraudster's global company, possibly also a lifetime guarantee on the products, and an impressive business card. The only catch is that it's all fake! The knives are massproduced Chinese rubbish, the leather is certainly no Nappa leather, and the "Persian" carpet is polypropylene. There never was an "original price", the brand logos are fake, the company doesn't exist, much less any quarantee, and the salesperson is working under an assumed name. The only thing that's real is the money that you have paid the fraudster.



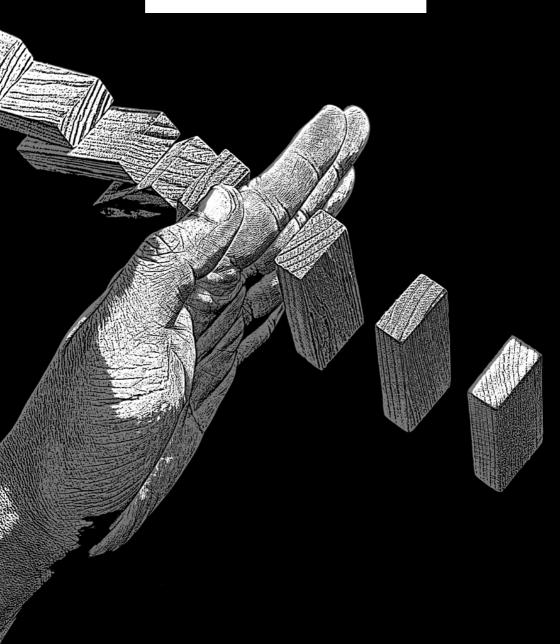
Never let yourself be talked into an impulse buy, no matter whether it's on the street, over the phone, or at your door. Don't let strangers into your home. Don't sign any contracts that you do not understand precisely, especially not under time pressure. Reputable firms will make you an offer that you can then consider in your own time and discuss with the people you trust. If you feel that you have fallen for a fraudulent scheme, ring the police and describe your situation. If you really have been the victim of fraud, be proactive in telling your friends and family what has happened. By doing so, you can stop the same thing happening to them.

5. Weapons



Whether or not private gun ownership increases personal security, or presents a risk, is a highly controversial topic. In this case, the police sees more risks than positives, and advises against arming yourself for your personal protection. In the broad sense, the law defines a "weapon" as any device (or imitation device) intended to injure or kill another human, such as a firearm, a blunt instrument, and certain knife-like weapons. The Swiss Weapons Act defines which weapons are available to whom, and which are essentially prohibited (such as butterfly knives), and governs weapons acquisition, carrying, transport and storage. Anyone who buys or already possesses a weapon must be extremely familiar with these rules, because breaches of the Weapons Act result in criminal prosecution. That said, there are items found in every household which, although they aren't designed to cause injury, they can be used for that purpose. These are known as dangerous objects and include, for example, kitchen knives, carpet knives, hammers and screwdrivers. Depending on the situation, golf clubs, frying pans and rolling pins can also be used as weapons, of course. Consequently, the improper carrying (both on one's person and in a vehicle) of dangerous objects is prohibited. Only a cook on their way to work is permitted to carry a chef's knife in their rucksack, and a tradesman must leave his hammer at home before going to the pub for a post-work beer. The only exception is a Swiss army knife, which you may (should?) carry at all times...

6. Civic courage



To conclude this booklet, we would like to look briefly at an issue that is only indirectly related to crime, but which is of the greatest importance to crime prevention: civic courage. Unfortunately, civic courage tends to attract media attention only when it doesn't work, or when the "have-a-go hero" is anything but, such as someone fearlessly getting involved in a fight without any realistic chance of winning, and being seriously injured as a result. Yet civic courage has nothing to do with fearlessness. It is found primarily in the build-up to situations which then become dangerous, so that no heroism is required at all. It is displayed by those who intervene on behalf of the community to help those who are being treated unjustly or even attacked physically. Civic courage is not shown primarily by the individual in an exceptional situation, but by the community in everyday life.

This community is formed by all Swiss citizens who are aware of the high quality of the values and legal structures they enjoy. Civic courage is not the dangerous hobby of a minority, but works only if it is practised by the majority. Indeed, it can and should be practised by everyone who find injustice fundamentally unacceptable, not just when they are affected personally. For these people, it is about **defending human rights,** such as the right to liberty, to equal rights, and to physical integrity. No person may be placed at a disadvantage because of their gender, origin, skin colour, sexual orientation, or political, religious or other views and beliefs, in either their professional or private life. Civic courage follows the well-known principle of "live and let live", and the golden ethics rule of "do as you would be done by". Ultimately, it is about human dignity. If you share these values and believe they should be defended vigorously, you are probably no stranger to civic courage. However, to respond correctly even in critical situations, please note the following six points.

1. Don't take risks

By that we mean avoid physical danger. Nobody wants you to become victim number two by trying to help victim number one. You should, however, take risks in which you aren't at physical threat, such as the risk of making a fool of yourself if there were a hidden camera somewhere. (And if there really is a hidden camera, you still have a legal right to your own image and can prevent any footage being broadcast.)

2. Ask for support

Immediately approach other observers and ask for their view of the situation. It may be that others are also willing to intervene, just like you, and there is safety in numbers.

3. Watch closely

What's going on? Who said what, and who lashed out first? To bring criminals to justice, it is important to be able to identify them clearly at a later date, and to be able to reconstruct exactly what happened. Precise observation is thus extremely important for witness statements.

4. Get help

If a situation is threatening to escalate or a fight is already in full swing, please call the police on 117. From the victim's perspective there's no doubt that it's better to call the police too soon than too late.

5. Look after the victim(s)

If you aren't able to intervene in a violent crime, don't walk away, but stay nearby to help the victim as soon as the have gone. Take a first-aid course so that you're well prepared not only for eventualities like this, but also for accidents in other areas of life.

6. Make a witness statement

Please make yourself available as a witness when the police arrive at the scene. You may have noticed a key detail that will lead to the attackers. The victim will thank you, because the best therapy for them is often to see their attacker punished.

Contact details of cantonal and municipal police forces

Police force	Webseite	Telephone
Kantonspolizei Aargau	www.polizei-ag.ch	062 835 81 81
Kantonspolizei Appenzell IRh.	www.ai.ch	071 788 95 00
Kantonspolizei Appenzell ARh.	www.polizei.ar.ch	071 343 66 66
Kantonspolizei Bern	www.police.be.ch	031 638 56 60
Polizei Basel-Landschaft	www.polizei.bl.ch	061 553 30 66
Kantonspolizei Basel-Stadt	www.polizei.bs.ch	061 267 82 84
Police cantonale Fribourg	www.policefr.ch	026 305 16 13
Police cantonale de Genève	www.ge.ch/organisation/ police-cantonale-geneve	022 427 56 00
Kantonspolizei Glarus	www.gl.ch/kapo	055 645 66 66
Kantonspolizei Graubünden	www.kapo.gr.ch	0800 80 30 50
Police cantonale jurassienne	www.jura.ch/police	032 420 65 65
Luzerner Polizei	www.polizei.lu.ch	041 289 24 44
Police neuchâteloise	www.ne.ch/police	032 889 90 00
Kantonspolizei Nidwalden	www.kapo.nw.ch	041 618 44 66
Kantonspolizei Obwalden	www.ow.ch/kapo	041 666 65 00
Kantonspolizei St.Gallen	www.kapo.sg.ch	058 229 38 29
Stadtpolizei St. Gallen	www.polizei.stadt.sg.ch	071 224 60 00
Schaffhauser Polizei	www.shpol.ch	052 624 24 24
Kantonspolizei Solothurn	www.polizei.so.ch	032 627 71 11
Kantonspolizei Schwyz	www.sz.ch/polizei	041 819 29 29
Kantonspolizei Thurgau	www.kapo.tg.ch	058 345 22 77
Polizia cantonale Ticino	www.polizia.ti.ch	0848 25 55 55
Kantonspolizei Uri	www.ur.ch/kapo	041 875 22 11
Police cantonale vaudoise	www.police.vd.ch	021 644 44 44
Kantonspolizei Wallis	www.polizeiwallis.ch	027 326 56 56
Zuger Polizei	www.zugerpolizei.ch	041 728 41 41
Kantonspolizei Zürich	www.kapo.zh.ch	044 295 98 00
Police de Lausanne	www.lausanne.ch	021 315 15 15
Polizia Città di Lugano	www.lugano.ch/sicurezza	058 866 81 11
Stadtpolizei Winterthur	www.stapo.winterthur.ch	052 267 51 52
Stadtpolizei Zürich	www.stadtpolizei.ch/ 044 411 74 44 praevention	
Landespolizei Fürstentum Liechtenstein	www.landespolizei.li	00423 236 71 11



S<??S(

Schweizerische Kriminalprävention Haus der Kantone Speichergasse 6 3001 Bern

www.skppsc.ch