Incidents that have actually taken place in Estonia as outlined by officers from Criminal Department of the Estonian Police and Border Guard Board.

It is recommended that these stories be used to inform and launch discussions with young people about the laws in Estonia.

Here you will find

Stories about security

The following are incidents that have actually taken place in Estonia as outlined by officers from the Criminal Department of the Estonian Police and Border Guard Board. We recommend that you use the stories to inform and launch discussions with young people about the laws in Estonia.

1. The MSN incident

Mum discovers that her daughter has been talking to a number of men on MSN about sex and that they have sent her clips filmed with web cameras and pictures of erotic and pornographic situations.

The police explain: In this case almost everything depends on how old the girl is who was sent the pictures. In any case, it's hardly the most pleasant of experiences, whether she's 10 or 17. According to § 179 of the Penal Code, providing anyone younger than 14 with pornographic material or a reproduction thereof or otherwise exhibiting or knowingly making it available to them is punishable by law.

What to do in this situation

The best thing to do would be to block the user(s) immediately. If you've already been sent erotic or pornographic clips, save them and the sender's details somewhere. Record their address and, if possible, save a log of the MSN conversation(s). If you're not using this function, either copy the conversation or take a screenshot of it.

Do as much as you can to save as much as you can about the details of a conversation, including the date and time it took place, any links/website addresses sent to you etc. Save the clips you've been sent, too.

Having done this, present all of this information to the police at your nearest station. It doesn't matter whether you go in person to the station or e-mail the information to them (which in some cases may be more convenient anyway). Since clips and logs are difficult to send on paper, note on your statement that you have them. Hold on to all of the files you have until the police have made copies of them and, if necessary, taken a copy of your hard drive.

It's a good idea to talk about this kind of situation with your parents or another adult you trust. If you don't have anyone like that, you can always tell the police – you don't have to be a certain age before you can come and talk to us. Don't forget to add your details to your statement – that way it's much easier for us to get in touch with you. You can contact us in person or by e-mail.

You should tell the police about these kinds of situations, because we are the only ones who can stop people from doing such things. You might block them, but they'll always find someone else to send their clips and pictures to. These people tend not to stop unless the police intervene.

The rule of thumb is: **block–copy–report**.

2. The password incident

Jüri tells the police that someone has hacked into his www.mail.ru and www.hotmail.com e-mail accounts and his user accounts on www.facebook.com and www.odnaklassniki.ru. His Apple laptop has also been infected as a result, and demeaning e-mails with a sexual undertone have been sent out in his name. The damage he's suffered is both moral and material.

The police explain:

A case like this constitutes two crimes:

1) § 217 of the Penal Code – unlawful access to a computer system by eliminating or circumventing a code, password or other means of protection; and

2) § 157-2 of the Penal Code – potential identity theft.

Although these actions are considered crimes, investigating and prosecuting them is very difficult. No material damage is incurred as a result, but the moral damage may be much greater than any financial loss.

Since all of the website addresses in this case end in either .ru or .com, finding out who has hacked into the accounts would require queries to be sent to Russia and the United States. Unfortunately, such queries are neither the quickest nor most effective means of investigation, and we often receive no response.

As a rule, however, such cases are solved.

Make sure your accounts are protected by strong passwords.

3. The game incident

Karl sends the passwords for his game Maplestory 11 to the MSN address of someone he knows on the Internet who's agreed to buy them from him. The agreement was that this person would transfer €28 to Karl's account. However, Karl hasn't received the money and the person he knows is no longer appearing online on MSN.

The police explain:

This is not a black-and-white case of a crime having been committed. If it were, it would be classified under § 213 of the Penal Code as computer-related fraud.

Of course, it would be great if such cases never came up. You should be extremely wary about anything you agree to buy or sell over the Internet – you can't see the other person and have nothing else to go on in terms of how trustworthy they seem than their words. Where selling passwords is concerned, it's almost like buying nothing – after all, you have no idea whether they'll work. The person who sells them could always deactivate them and demand more money from you (as happened in this case).

If you've fallen victim to this kind of scheme, record the following material:

1. conversations with the seller – the agreement to buy/sell whatever it is, as well as any later discussions about the transaction (on MSN, via e-mail etc.). If you encounter problems, it's best to make any claims and complaints by e-mail, since they're much easier to reproduce. You need to make sure you collect and save your e-mails and those sent to you by the seller; and

2. documents proving that money has changed hands.

You should then take or send all of this material with a statement to your local police station so that an investigation can be launched. Try to include as many of the facts of the case as possible in your statement – there can never be too much factual information.

We recommend that you ask an adult for help putting your statement together. If you don't feel you can, come and talk to us yourself and we can help you write your statement.

Whenever buying or selling something online, save all of your conversations, e-mails etc. until the transaction is finalised and everything has worked out the way it should.

4. The car incident

On the www.osta.ee site, an unknown person has used the details of a user called Jänes to buy a car in an auction for €4800. The fine for ultimately not buying the car is €1000. But 'Jänes' didn't even take part in the auction, or buy the car.

The police explain:

There's not much to add here, coming after the case with the game passwords above. It's an example of someone falling victim twice: they're already the victim of one crime, but they then face other problems (they're issued with fines). SMS loan fraud is much the same – proving that you didn't borrow the money is very difficult and time-consuming, and can't even always be done. And all the while the interest on the amount you borrowed (or rather didn't borrow) is growing.

5. The whodunit incident

Someone has been using Jane's mobile phone without her knowing. 45 calls have been placed to the special rate number 15154 at a total cost of €146. At the time the calls were made, Jane had three friends over – Liisa (13), Peeter (12) and Siim (10).

The police explain:

This could again be a case of computer-related fraud under § 213 of the Penal Code. The best advice here is never lend your mobile to someone else, not even if you know them well.

The logic behind it is simple: calls made and text messages sent using a mobile phone cost money. At most it'll only take until the start of the next month for your parents to get the bill, and then there'll be trouble. You should be particularly careful phoning or texting any of those five-digit numbers. There's no such thing as a free lunch, and there's no such thing as free games and ringtones. And extricating yourself from these services once you're in their grip can be very difficult.

Bear in mind, too, that there's usually some small print somewhere saying that if you reply to an SMS or tick a box somewhere online it means you've agreed to the terms of an agreement, in which case it can't be called a crime. It then becomes a civil matter, in which case the victim or the person representing them can take the case to a civil court. But given the complexity and cost of proceedings (you have to pay to submit a civil claim) and the damages normally involved, most people tend not to take the case to court, since it's ultimately cheaper to just pay the bill. And that's usually what the people behind these schemes bank on.

6. The bill incident

Rein loses his Nokia mobile. Some time later, he receives a bill indicating that a transfer of €480 was made to a www.rate.ee account on the day he lost the phone.

The police explain:

This could well be a case of theft. If your mobile is stolen, you should close it as soon as you realise that it's been taken – that way you should avoid any financial damage.

In this particular case it's pretty easy to work out via www.rate.ee who the person was who made the transactions. This could lead to the person who actually stole the phone. It's not impossible that Rein himself is behind it all, even though he said he lost the phone.

7. The stolen phone incident

Kati is going to Finland, but since calls cost a lot more there, she lets her friends know that she's coming and then doesn't make any more calls. The next day she returns to Estonia but discovers when she gets home that her mobile's no longer in her pocket. She uses her old mobile to call Tele2 and asks them to close the card. She's told that the last calls made from her mobile were to Estonia. Some time later, she receives an SMS from Tele2 saying that her €64 limit has been exceeded – and that in fact the balance of her account is €1130! Kati can't say for sure when or where her phone was stolen. In total she's facing damages of €1122.

The police explain:

This is similar to the previous case. It's worth noting here that the limits you set yourself aren't always of help – particularly if you and your phone are outside of Estonia.

The simplest recommendation here is to always make sure you have all of your belongings on you or with you. Remember that a mobile has material value and that calls made with it have to be paid for. Keep your phone somewhere safe – if it's in a bag, make sure the bag's closed (or even better, locked); if it's in your jacket, stick it in a pocket with a zip on it. Open bags, back pockets of jeans, open pockets in jackets and such are the worst places you can keep your phone, since they'll be an obvious target for anyone looking to steal one.

8. The bankcard incident

Dad opens an account for his son in Swedbank, including a card. The boy has no money in the account, so when he loses the card dad doesn't worry about letting anyone know. But suddenly huge sums are being run up on the card, and a bunch of transactions have been made through the account.

The police explain:

The moral of the story is: keep hold of your valuables. A bank card is plastic money, and a SIM card is money waiting to be made. Never carry your account number, bank card and PIN around together. Never tell anyone what your account number is, either – even if they offer to pay. Giving someone free rein to make use of your account could leave you having to repay SMS loans, or criminals could use your account to store money they've obtained from crime. And always say 'no' if someone asks you to open an account and then give the account cards to someone else to use.

Recommendations for parents

- Talk to your kids: tell them about the dangers the Internet poses.
- Explain to your kids that with mobile phones every call and every SMS costs money – don't assume that limits will ward off enormous bills!
- Trust your kids, but check what they're doing. If you've set up a bank account for them, keep an eye on what's happening with it.
- Talk to your kids in a way that generates trust. If they've lost something or had something stolen, help them deal with the situation. If they know you'll just get angry, they'll hide what's happened for as long as they possibly can. If they've lost their phone or their bankcard, it's important that they're closed immediately – delays of a few days or even a few hours could end up costing you dearly.

Contact: Anu Baum
anu.baum@politsei.ee