Security Policy

At LNAday OÜ . we understand how important the security and confidentiality of your information is to you. Our aim is to protect your information on the Internet in the same way as we would through our other channels such as over the phone.

To ensure the highest level of security of information passing between our customers and the company, we use what is known as 128 bit SSL. This is an encryption method that scrambles information while it is moving from one source to another to prevent the information being viewed or tampered with.

1. SECURITY MEASURES.

We have an integrated system of industry best practices and technologically advanced safeguards that includes:

• SSL and encryption; • Firewall; • Cookies; • Monitoring; • Automatic logout.

SSL and encryption: we use an industry-standard technology called Secure Sockets Layer (SSL) on our account services websites to encrypt the information flowing between your computer and our servers. Encryption works by scrambling words and numbers before they travel across the Internet so they can't be read or altered.

Several levels of encryption are available. A higher number indicates more secure communication. Browsers that support 128-bit encryption or higher currently offer the best protection.

Firewall: a firewall is a combination of hardware and software deployed to control the information that can pass from the Internet into our internal systems and servers. Firewalls enforce a set of rules intended to bar intruders and viruses from gaining entry.

Cookies are small text files that are sent to and stored on your computer, smartphone, tablet or other device for accessing the internet, whenever you visit a website or use our on-line apps. More general information on cookies can be found on aboutcookies.org. This includes information on how to disable cookies.

Monitoring: we continually monitor our systems for evidence of attempted break-ins. Our monitoring methods combine internal resources and security companies we pay to help safeguard your information.

Automatic logout: the automatic logout is intended to protect your account information from passersby if you're interrupted and leave your computer before logging out. Typically, you'll be automatically logged out 20 minutes after your last click in a secure session.

1.1. Security threats are ever changing.

We use intensive testing procedures and other safeguards to verify that customer information is protected. But no security system is foolproof. Please be sure you're comfortable with our security measures before accessing your account online.

1.2. Security measures you can take.

You can take numerous actions to increase your Internet security. Some basic security measures are listed below:

• Use a browser with 128-bit encryption or higher; • Make sure you're on a secure page; • Log out and close your browser; • Clear your cache.

Use a browser with 128-bit encryption or higher. To enter the account service areas of our site, your browser must support minimum 128-bit encryption.

Make sure you're on a secure page. When viewing account information online, you'll know that the information being transmitted is being encrypted and secure if the "locking" symbol of your browser shows a closed lock. Your browser will always display this lock in the same location. Typically, it's in the lower right of the browser window, but not all browsers show it in the same place. Find it on your browser and always check for it in that location when inputting or looking at confidential information.

You can also look at the address box (URL) to see whether http:// has changed to https://. The "s" indicates your connection is secure. However, you can't trust this indicator alone if you've clicked an email link because some "phishing" scams have managed to fake the "https" to make the URL look secure.

Log out and close your browser. If you leave a computer without logging out and closing your browser, someone else could use the browser's back button to view information you entered.

The user ID and password you use to access account information on LNAday OÜ . website are protected separately by our site's security, which clears them from your browser as soon as you've logged in.

Clear your cache. As an additional precaution after visiting any secure site, you may wish to delete any page images your browser stored to your hard drive. These page images are called "cache". Your computer uses cache to make your experience faster by loading images from your hard drive rather than downloading them repeatedly from the website's server. Your browser's Help section should have instructions detailing how to clear your cache.

2. MEASURES FOR THE "PHISHING" PREVENTION.

Phishing it's any email that seems to be from a legitimate business but is really intended to steal personal information.

Have you ever received an email from a business asking you to provide personal information like your personal identification number or account number or asking you to click on a suspicious web link? Chances are it was a scam by someone trying to steal your identity for fraudulent purposes.

Phishers bait their hooks with an email designed to look like it's from a bank, retail or auction site, or some other business you may have an online relationship with. The message typically claims there's a problem with your account and asks you to click a link in the email and return to their site to confirm your account number, credit card information, password or other sensitive information. Sometimes the e-mail simply asks you to download an attachment which may be infected with a virus or spyware (see Combating viruses and spyware below).

The link takes you to a site cleverly designed to look like the business's website, but any information you enter is captured by the phisher, who may use it to steal your identity, make purchases using your credit card or drain money from your accounts.

2.1. How to avoid being hooked by phishers.

Develop a healthy skepticism when reading any email that asks for sensitive information and take a couple of simple steps to protect yourself.

Retype the URL. Phishers are very sophisticated in their use of design and technology to make their email lures look legitimate. The URL for the link in a phishing scam email usually appears to be a company's valid Web address. If you click the link, you're redirected to the phishers' phony site. However, if you type the displayed address into your browser rather than clicking the link, you can avoid being redirected.

Call the company. LNAday OÜ . will never ask for personal financial information from you in an email, and we believe most reputable financial services companies won't either. If you have any doubts about the legitimacy of an email, call the company that sent it.

Banks and financial companies typically have phone support in addition to their websites. A quick phone call to the customer support department can let you know if the "problem with your account" is for real.

Stay informed. Phishing scams become more complex as the phishers try to stay ahead of the people trying to stop them. You can keep learn more about the latest phishing scams at www.antiphishing.org, a website hosted by a group trying to eliminate identity theft and fraud related to phishing.

3. USING EMAIL SAFELY.

Email has become part of the very fabric of our lives. It lets us communicate quickly and easily with friends and family across town or across the globe. But don't let email's convenience make you forget about its potential dangers.

Following a few simple guidelines when using email can help protect you and your computer from identity thieves and unscrupulous businesses.

3.1. Treat email like a postcard.

Email is not a private method of communication. Anyone with a certain level of technological know-how can read what you send. While it may seem unlikely that anyone would bother trying to read your emails in transit, it's wise to err on the side of caution.

Avoid writing anything in an email that you wouldn't be willing to write on a postcard and drop in a mailbox. That means no personal financial information like account numbers, Social Security numbers, tax identification numbers or the equivalent personal identification numbers in your country, passport numbers or passwords.

3.2. Avoiding email viruses.

Hardly a week goes by without a major news story about a virus circulating on the Internet by email. These viruses typically arrive in the form of an attachment with some enticing invitation to open it.

If you open it, the virus can do almost anything–from sending out copies of itself to everyone in your address book to crashing your computer completely. Your best bet is to delete the email and the attachment immediately without opening them, especially if you don't know the sender.

Viruses are tricky though, and the emails they're attached to can seem to be from someone you know and trust, someone who would never knowingly send you a computer virus. So, it pays to be suspicious of attachments in general.

Before you open an unexpected attachment from a friend or family member, you may want to send them an email or give them a call to make sure they sent it.

3.3. Dealing with spam.

Unsolicited email–commonly called spam–is a growing problem on the Internet, both for recipients and for companies trying to use email to communicate with customers. Low mortgage rate offers, porn site solicitations, phishing scams and ads for merchandise are all forms of spam.

Use a spam filter. A good first line of defense against spam is spam-blocking software. Many email programs like Outlook or Eudora have built-in spam protection tools. Likewise, your Internet service provider may include a spam-blocking system bundled with their service. If these options aren't available to you, look into purchasing and installing spam-blocking software for yourself. These systems do a reasonable job of reducing spam, but they aren't 100% effective.

Delete without opening. When you reply or even open a spam message you may be confirming to the spammer that your email address is active. That's likely to mean more spam will be coming your way as the "good" address gets passed around among spammers.

Unsubscribe with caution. If spam comes from a company or individual you don't know, following the instructions to "unsubscribe" or be removed from the mailing list isn't likely to stop the spam. Your request will probably just confirm to the spammer that the address is active, and your address is more likely to be added to other lists rather than removed from any.

However, if what you think of as spam is coming from a company you have a relationship with, consider the possibility that they think you want to receive what they're sending. They might not realize they're annoying you with these emails because you may have forgotten you signed up for a newsletter or special offers by email. Legitimate businesses that want you as a customer will generally provide you with an email address to contact them to have your name removed from email lists.

Report spammers. Internet service providers often make ongoing efforts to combat spam on their systems. By reporting spam when you receive it, you can sometimes help service providers thwart spammers in the future. Contact your provider to find out if they have procedures in place for you to report spam.

4. COMBATING VIRUSES AND SPYWARE.

A virus or spyware on your computer can do more than just crash your system or delete files. More insidious strains can present a serious threat to the security of personal information.

A virus is a program that enters your computer without your knowledge and attaches itself to other files, replicating itself and spreading. Spyware is similar in that it invades your computer without your knowledge, but it also monitors your activity. In some cases it may report this activity back to the person who originally wrote the program.

Keeping your computer free of all unwanted programs is an important aspect of making sure your personal information is secure.

4.1. Be cautious when downloading files.

Be aware that whenever you download software or application files from the Internet, you could be allowing a Trojan horse into your system. A Trojan horse is a file that has undesired components like viruses or spyware hidden inside.

These programs vary in the amount of damage they do. One might simply annoy and frustrate you by resetting your browser's home page and not letting you change it back. Another might capture your ID

and password as you log into a financial site and then relay that information back to the source, where it may be used to steal your identity.

Be as certain as possible that you can trust the integrity of the source before downloading anything. However, you don't have to download something for malicious programs to find their way onto your system. Some of them can sneak onto your computer without any action on your part beyond visiting a website that hasn't taken appropriate steps to prevent hackers from triggering these "drive-by" downloads. Our site has security measures in place to combat this kind of activity.

4.2. Keeping your system clean.

Antivirus and antispyware programs that seek out and destroy spyware are available to help keep such programs off your system. But be aware that viruses and spyware aren't easy to eliminate.

For instance, spyware programs typically hit your computer in clusters rather than single programs. So when spyware A invades your machine, spyware B, C, D and E may also sneak in and find a place to hide. In addition to watching you, these programs watch each other. If spyware A gets deleted, spyware B reaches out to the originator and grabs another copy. So it's important to be disconnected from the Internet before trying to clean these files from your system.

Our Internet security expert recommends running your antispyware and antivirus programs several times in succession. Each run may be able to peel off layers of "masks," allowing the programs to work in tandem to target and destroy spyware and viruses that have been hiding. As a final step, restart your computer. Then run your anti-spyware and antivirus programs once more.

This process may seem like overkill, but many experts believe it's worth the effort to keep your system clean. If you'd rather not do all of what's described above, it's a good idea to run the anti-spyware and antivirus programs at least once.

5. USING PUBLIC COMPUTERS WITH CAUTION.

While airports and other venues with public computer terminals offer convenience, using them could compromise the security of your personal information.

You're on vacation and haven't been able to check email for a week. You stop for a cappuccino and notice a computer terminal in the corner of the coffee shop. It has Internet access and you decide to check your email and glance at the headlines on your favorite news website. No problem so far.

Then you decide to visit your bank's website, log in and check to see if a couple of recent transactions have cleared. Is that a good idea? Probably not since you're using a public computer terminal.

There's no way for you to know what kinds of spyware programs are installed on public terminals. The computer may contain key-tracking software or other invasive programs installed by someone who used the terminal previously. Those programs could help someone steal your identity if you're typing in personal information like an ID and password for online access to your bank account.

Given the ease with which spyware and other treacherous programs can imbed themselves on a personal computer used only by you, it's wise to be extra cautious and never access personal financial data from a computer used by the general public.

Certain information and statements made herein have been derived by third party sources. While we consider that information to be reliable, we give no assurance that such information or statements are accurate or complete.