Tips on cyber security when away from home

On a business trip - and especially when on holiday - it's easy to overlook the security measures that you instinctively take at home. Kaspersky Lab's experts share advice on what you need to do to make sure your hotel Wi-Fi access is secure, you're safe to buy tickets online and how you can respond if your device is lost or stolen...

On a business trip - and especially when on holiday - it's easy to overlook the security measures that you instinctively take at home. Kaspersky Lab's experts share advice on what you need to do to make sure your hotel Wi-Fi access is secure, you're safe to buy tickets online and how you can respond if your device is lost or stolen.

Hotels, restaurants, and business centres sometimes offer free tablets to their guests. While working on these devices, users tend to leave a lot of private information that could potentially be used by cybercriminals. You have no way of knowing if a keylogger or other malware has been installed to capture your keystrokes, including user names and passwords, as you type. These machines should be used only to visit public information websites, never for online shopping or for business purposes, such as editing documents or connecting to websites that require a password.

In 2014, Kaspersky Lab released information about the Dark Hotel targeted campaign, which used an effective intrusion set on hotel networks, even to systems that were believed to be private and secure. Cybercriminals waited until, after check in, the victim connected to the hotel Wi-Fi network. Then they tricked the target into downloading and installing a backdoor that pretended to be an update for legitimate software. Once on the system, the backdoor downloaded more advanced tools to collect data about the system, steal all keystrokes, and hunt for cached passwords in browsers and other private information.

The 'update' could prove to be malware

It's always a good idea to keep your software updated. But when on a trip, make sure you download updates directly from vendor websites: if your computer tells you that your software needs updating, don't click on a button to download and install the update there and then; the 'update' could prove to be malware.

If you need to use internet for something that involves sensitive information take care to use a safe connection:

- Avoid using public Wi-Fi, especially if the network is not password protected: hackers may set up Wi-Fi hotspots in public places like airports to intercept your data. Often these will have official sounding names, so it's sensible to establish the exact name of the legitimate Wi-Fi service. It's recommended to use only password protected networks.

Even if the Wi-Fi password is freely available to everyone, it still provides protection. That's because this common password is used to generate unique session keys for each user, so your data can't be decrypted by anyone else, even if they know the Wi-Fi password.

- Use a Virtual Private Network (VPN) when accessing the internet and disable wireless services and network connections when not connected to the VPN to prevent unauthorised access. Websites and email services that use https and display a locked padlock in your browser encrypt your data automatically. However, it's a much more secure practice to encrypt all traffic coming and going from your computer when using a public network by using a VPN. Many businesses have their own corporate VPNs, or you can subscribe to a VPN service (such as Black Logic, HotSpotVPN, Proxpn or StreamVia) for a short period or annually.

If you go online to buy tickets for a show or book a hotel in another city, consider the following:

- Make sure the service that is about to handle your money is secure (green padlock, encrypted HTTPS connection);
- Run a solid anti-virus program with a built-in safe money protection feature;
- Have a unique password for each of your accounts and implement some form of two-factor authentication on whatever site you are using. This way, you will have to confirm any logins using an SMS or email-based security code. If you get a two-factor notification when you aren't attempting to login, then that is a pretty good indication that it is time for a security scan of your computer and a new password (because it means someone probably has your password and is trying to access your account); and
- Use some sort of transaction guarantor, like 3D Secure or Verified-By-Visa, which will require another one-time password from you before the transaction can go through.

Physical security should also be considered as your data is at risk any time you leave your computer unattended while travelling. Devices are also susceptible to being lost or stolen. So sensible precautions include setting a login password if there is not one already - although this only offers a low level of protection; requiring a password to be re-entered after a relatively short idle period. Also it's good to disable booting from a CD or USB drive in the BIOS to prevent hackers bypassing a login password, and then setting a BIOS password to prevent the BIOS settings being changed.

Take precautionary measures by familiarising yourself with the anti-theft features available to you on whatever device you are using. For example, the Kaspersky Phound! free application for smartphones or tablets - as well as Kaspersky Lab's consumer products, including Kaspersky Internet Security Multi-Device, - can help with a number of features, including locating the device on a map using GPS, GSM or Wi-Fi networks, turning on an Alarm feature that continues until the owner enters a secret code or even removing all personal data.

"A lot of people travel nowadays with their smartphones, notebooks and tablets, or use devices provided to them on the trip. When quickly packing a bag for a trip, in a hotel or in an airport, it's easy to overlook even the simplest security measures, such as backing up files or encrypting vital business data. Then there are threats like losing passwords or getting infected by cybercriminals via untrusted public charging stations that use a USB connection. You should take precautions on your travels just like you would at home," said Stefan Tanase, Senior Security Researcher, Global Research & Analysis Team, Kaspersky Lab, during his presentation at Kaspersky Lab's Cyber Security Weekend conference, held in Lisbon in April 2015.