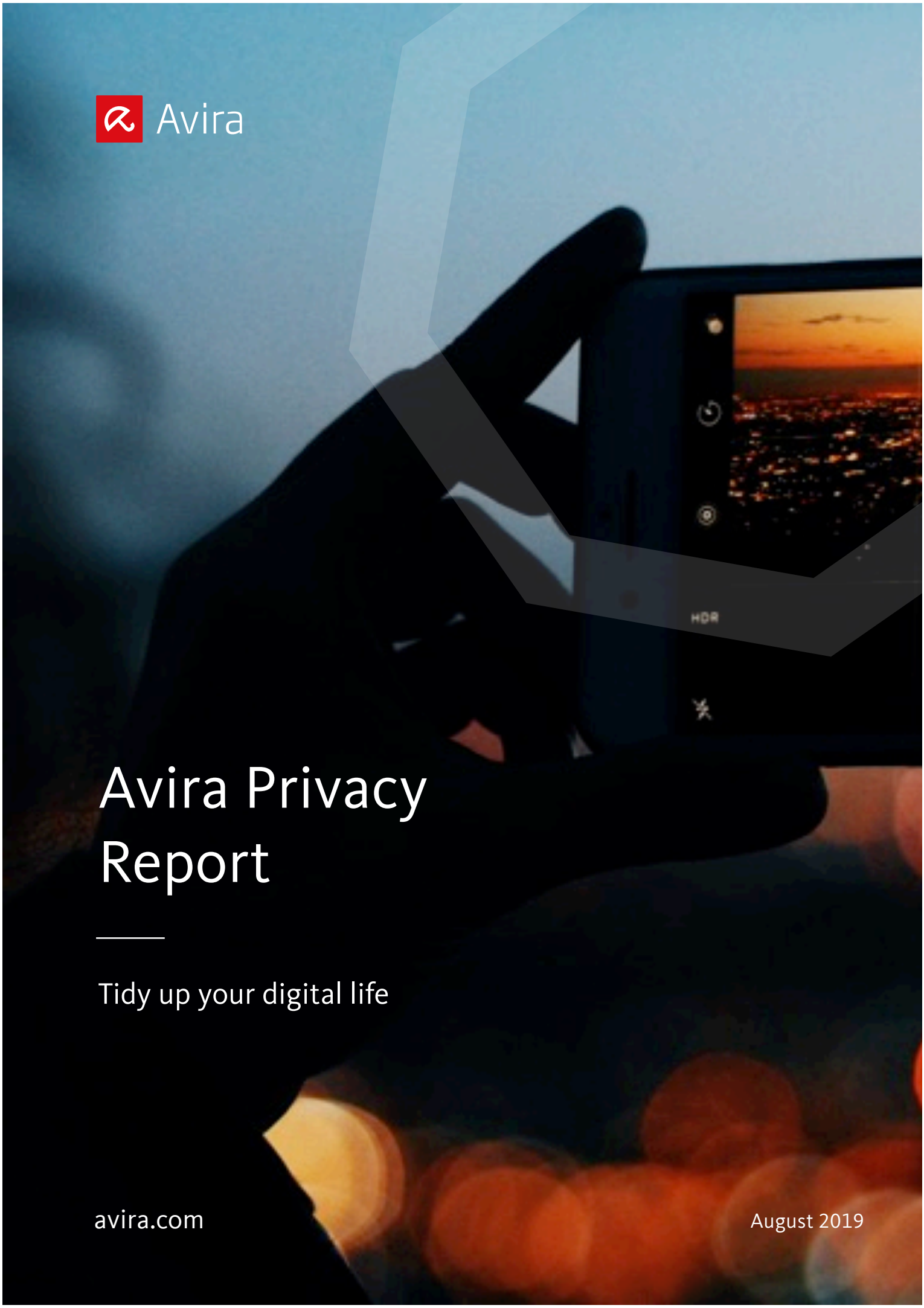


Avira Privacy Report

Tidy up your digital life

avira.com

August 2019

Introduction

When it comes to online security, summer is no vacation.

Instead, the threats and the risks go mobile, as people take their devices with them in their quest for new experiences and new places.

By midyear, our research showed that old, repackaged threats are more – just by numbers of blocked attacks – prevalent than those headlines grabbing zero-day attacks.

While traveling, it's also a good time for people to get their digital habits in order – staying up-to-date, moving beyond a "sticky note" system of password management, and using a VPN to get better security and content out of free Wi-Fi networks.

Escapism can be part of an idyllic summer vacation – but not when going online. As a connected individual, being careful about what is clicked on and where private data is entered, are security recommendations that will always be in season.

Safe surfing,

Travis Witteveen,
CEO Avira

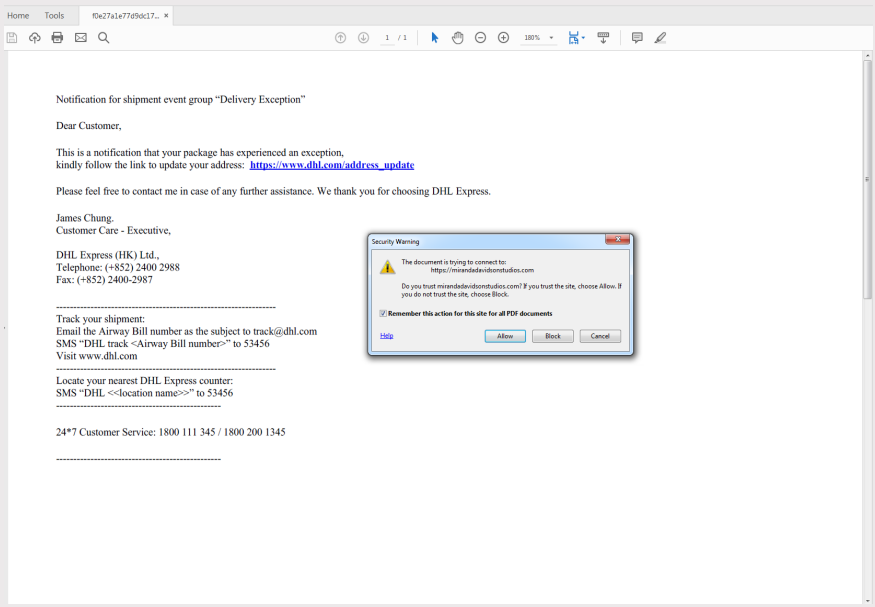
Summertime threats (1)

As summer rolls around, so do the incoming threats as the bad guys work to get into your devices and make money out of them. While we are often attracted to the new and innovative – in fashion, vacation hot spots, and technology, it's worth pointing out that the malware infection vector for 2019 is a mixture of old and new.

Phishing Attack (literally but figuratively real)

Phishing emails are still one of attackers' most effective methods. This usually happens during vacation time when people are caught off-guard looking, skimming through emails being prone to such threats.

An example would be this one - a highly advanced phishing sample recently spotted by our engines. It appears to be a DHL delivery note, written professionally - unlike common phishing attempts, the URL in the document appears to be the DHL website. But, in fact, this is actually a malicious website (as shown in the image) created to trick people into giving up sensitive information after clicking on the link.



Summertime threats (2)

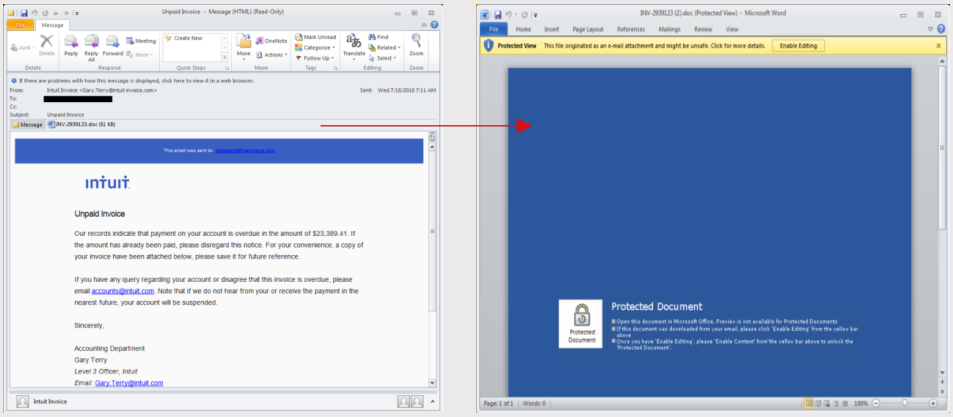
EXP/CVE-2010-2568 (Old dagger but still a gold digger)

Old windows vulnerabilities can still be a gold digger. This is an old Windows vulnerability where Windows shell allows attackers to execute arbitrary code via a specially crafted .LNK or .PIF shortcut file. When the default auto play is enabled in Windows, this is enough to trigger the malicious code by only previewing the file containing the exploit – that is often placed on an USB stick.

Trickbot (Evolved with a new skin)

Recently, Trickbot, a banking trojan, proved to be the most wanted malware because of its new advanced wave in the wild affecting more than 250M emails. This new version, knows as TrickBooster, is signed with a valid certificate and is very feature-rich and advanced:

- Memory-based powershell spam mail-bot module
- Browser Grabber module for cookie and data extraction
- WebInjects for popular banking websites to steal credentials
- Can spread laterally via famous EternalBlue exploit
- WalletStealer capabilities
- Stealing credentials from installed programs, such as Outlook, converting the infected computer to an email spam node
- Heavily encrypted and obfuscated
- Continuously updated via C&C servers running primarily on exploited routers



Security pointers:

Security pointers:

- Have up-to-date antivirus software
- Update your Windows and other installed software, replace old outdated software with newer versions
- Avoid USBs from unknown origin, they could be infected
- Avoid opening files/links from unknown/spam emails. Also, do not provide any credentials to unknown links or sources or download files attached in these emails.
- Keep browsers up-to-date.
- Change your credentials frequently

"It's not just the new and shiny zero-day threats that are a concern. Because security is not always convenient, many people are slack and a bit careless when it comes to doing the basic steps to protect their digital lives."

Alexander Vukcevic,
Director Protection Labs & QA

Updates are mandatory

Stay up to date

Running out-of-date software opens up vulnerabilities that have been exploited to target everything from individual devices to corporate networks.

In particular, unpatched software opens up your device to hackers wanting control of your device, access to your private data, and the ability to also step into the devices of your connected friends and family members.

According to a recent Avira report, **some of the biggest software vulnerability patches/important updates in the past months have been with Google Chrome, Java 8, and the Adobe Flash Player plug-in 32. In addition, false alerts for Adobe Flash Player updates are a known strategy for distributing malware.**

Keeping fully updated is also a numbers game. Typically users are unable to successfully research and apply updates for all the various apps on their devices – so they just don't do it. Confusion over real vs. fake updates has supported the use of automated software updaters that take over this task of searching for and applying patches

Performance matters

Devices and suitcases can have a lot in common. In particular, their owners tend to accumulate stuff in the corners which slows down daily life and limits performance.

That's why cleaning up is imperative for a good digital experience – so, erase those unnecessary confidential files permanently and make room for new ones.

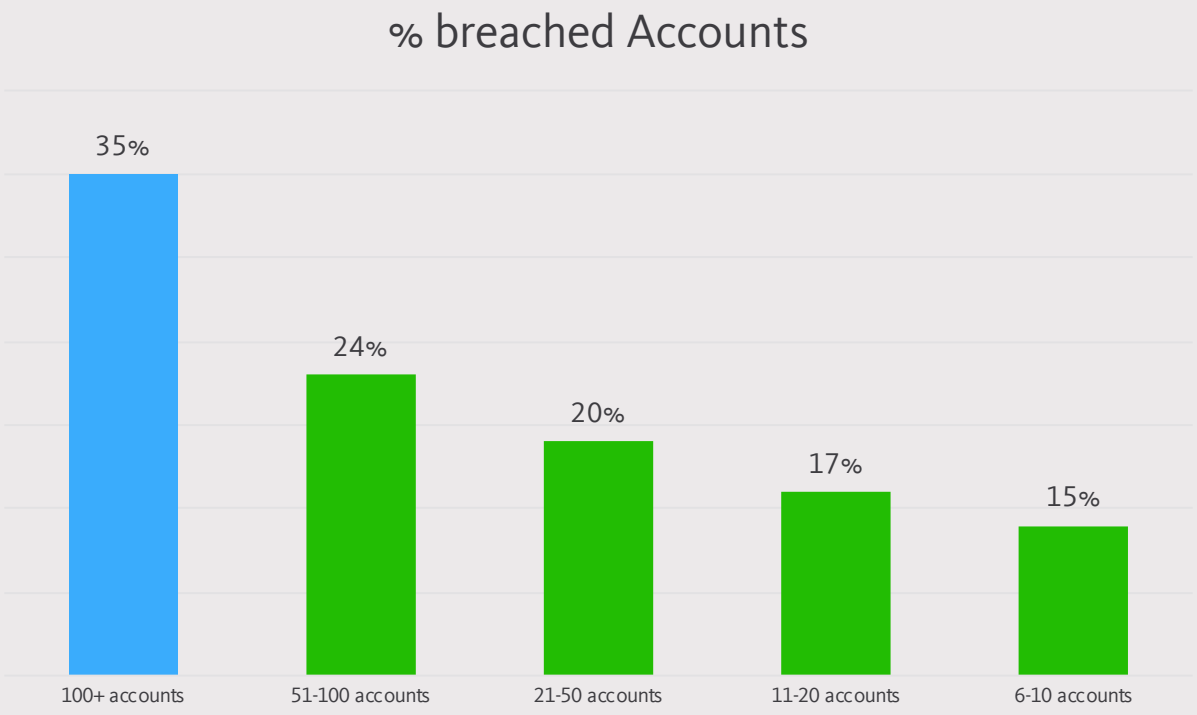
From January to end May, the total memory space saved for Windows users reached an accumulated 651,714,335 MB. From February to May, estimates for saved space for Android users came to 321,118,640 MB.

The minutes saved by users during the more speedy system boot-up in the mornings are not included here.

Time to hit the breach

Sun, sand, and data breaches. Data on the frequency of account hacks and breaches shows a basic fact of life: The more accounts one has, the much higher risk that any one of them might be hacked. This primarily comes from the limited memory of humans and recycled passwords. **People with 1-5 accounts have a 14% chance of an account being breached – a percentage that goes up to 21 when the individual has over 30 accounts.**

It is difficult for most people to remember secure passwords that are over eight characters long and contain a mix of letters, numbers, symbols, and capitalization. So they don't – and they simply recycle one password – or a simple variation of it – across all of their accounts. The problem comes from when one account is hacked – the problem spreads to all accounts.



*Data collected by Avira on January 1st, 2019 – May 31, 2019

Accounts Security

There is absolutely nothing people can do to secure themselves against the newest trend in leaked and hacked passwords – but they can make re-securing their accounts easier. Many of the latest leaks have been through organizations not setting up their cloud data storage accounts securely. Where entry is not protected by an effective password and the data is unencrypted – something bad can and does happen.

In this case, consumers can fight a defensive battle, checking at www.haveibeenpwned.com or to see if their password has appeared on a dark-web list. Or, if they are using a password manager, they can receive an alarm in case their accounts were involved in a data breach. Moreover, a password manager can help on generating strong and unique passwords for all accounts and on memorizing them safely.

Passwords are not going away soon

The establishment of the world wide web consortium (W3C) to make a new web standard called **WebAuthn** raised some hopes that passwords would go away. However, this will likely start just as a second-optional factor for authentication.

The main issue now is that WebAuthn is device linked and would require not only registration for each service, it would also require registration for each device.

“Think of the organizational overhead to keep track and understand which of your services is registered with which of your authenticator devices. Besides these conceptual issues, **data encryption cannot be done with WebAuthn**”, explains Tom Gaiser, head of the Avira Identity Protection Unit at Avira. “The best way to do this is to use a password that only the owner of the data knows - like the Master Password on a password manager.”

Surf anonymously and securely

A VPN, or virtual private network, establishes a secure, encrypted connection between physically separated devices. It's a big step forward in privacy from unencrypted HTTP data packets. We often describe HTTP as an openly readable vacation postcard and a VPN as a certified, registered letter – where each party has to sign off for the delivery.

Seasons matter for VPN use
Recent Avira research found that seasons do make a difference when it comes to VPN use. There is a distinct increase in the number of users during the summer months and also a shift towards users using a VPN more often on their smartphones. Our American survey found that **51% of respondents used a VPN on their smartphone – almost as much as the 56% using a VPN on their laptops.**

Typical use also corelated to the summer months with **66% using it for more secure connections for banking and for communicating via public Wi-Fi networks and 65% using a VPN to circumvent geo-IP restrictions to view or stream website content while they were outside of the USA.**

*Source: Avira Online Survey (multiple choice option) with 2519 respondents, aged between 20-65 years (US – January – February 2019)

The connected world

In the first five months of 2019, **2.99 million home networks** were scanned with Avira's free Home Guard app.

22.8 million devices were connected to these wireless networks, including smartphones, laptops, as well as smart TVs, gaming consoles, smart thermostats, baby monitors and other smart home IoT devices. On average, across the world, there are **7.91 connected devices per home network**.

On a global level, the UK was in the lead with 12.44 devices per network. Germany was below the average with 6,19 connected devices per network, as was France with 7.02 devices per network. Clocking in above the global average was the **United States with 10.41** and Italy with 8.95 devices/network.

The secret life of TVs

TVs are often the first connected IoT device brought into a home – but very few people know what these devices do under their very eyes.

Smart TVs came under increasing scrutiny earlier in 2019 when hackers used 72,000 Smart TVs to send viewers messages promoting YouTube star PewDiePie. Smart TVs have proved to be easy targets, with even unsophisticated hackers being able to connect to them remotely. Intruders have been able to change channels, turn up the volume, and play disturbing or relatively harmless content (such as the request to subscribe to PewDiePie).

Smart TVs also raise privacy concerns by collecting and sharing personal data from consumers. While people expect their laptops and smartphones to gather user data, **internet connected TVs also collect significant amounts of data**. Information on TV viewership habits, program choices, and other kinds of information is then sent to TV manufacturers and their advertising partners – often without the awareness of consumers.

Summertime survival suggestions (1)

Summer is a special time where we look forward to familiar faces and distant countries – and even plan these events months ahead of time. Nowadays, our technology goes with us as laptops, mobile phones and tablets finding a way into our baggage. To avoid headaches during your vacation, here are some basic pointers:

Get your vaccinations up to date

- Antivirus – Have a reputable, independently tested security app installed on your device which will secure you from the new – and the old – threats.

- Updates – Stay ahead of threats by having a fully patched device. The easiest way to do this is to have a software updater installed. This takes the responsibility for finding and installing the latest updates for the dozens of apps on your devices.

Give your brain a break

- Password manager – Stop recycling passwords – and don't bother trying to remember secure and unique passwords for all of your devices and online accounts. Just get a password manager so you only have to remember one secure password – and let this solution take care of creating, remembering, and syncing secure passwords across your device portfolio.

Go everywhere in style

- A virtual private network can go with you on all devices – not just stay at home on your desktop. A VPN lets you communicate securely on those insecure public networks and lets you pick your own GEO-IP, opening up content regardless of where you might actually be. Without a VPN, don't even think about entering in any private data over a public Wi-Fi.

Summertime survival suggestions (2)

Look out for the phish

- Phish – specially crafted deceptive emails or websites designed to look like they came from the real source – are a big business. Cybercriminals use them to distribute ransomware, infiltrate political parties, and fool individuals into giving them passwords and login credentials.

- Click with care – Take a look at emails and website carefully. Is the sender address correct? Are the links in the encrypted HTTPS? Does it feel correct? Clicking on suspicious email links is also an easy way to pick up a ransomware infection.

- Hold your data – Don't enter data into links and attachments sent to you via email.

Put your smart devices on a leash

- Find out what your smart devices are doing when you aren't around. Use the available free apps to find out just who is on your home network, who they may be talking to, and if they are communicating securely.

Be a happy skeptic – **The biggest factor in your security is you**. While an antivirus program will filter out the vast majority of the bad stuff – and updaters and password managers will make life easier and more secure – don't forget that you have a role to play. This is where your inner sense of skepticism is incredibly important – take it with you on vacation. Your online health depends on it.

About Avira

Avira protects people in the connected world – enabling everyone to manage, secure, and improve their digital lives.

The Avira umbrella covers a portfolio of security and performance applications for Windows, Android, MacOS, and iOS. In addition, the reach of our protective technologies extends through OEM partnerships. Our security solutions consistently achieve best-in-class results in independent tests for detection, performance, and usability.

Avira is a privately-owned company that employs 500 people. Its headquarters are near Lake Constance, in Tettnang, Germany, and the company has additional offices in Romania, India, Singapore, China, Japan & the United States. A portion of Avira's sales support the Auerbach Foundation, which assists education, children, and families
in need.

For more information about Avira visit www.avira.com.

avira.com