ALLIANZ GLOBAL CORPORATE & SPECIALTY®

CORONAVIRUS: STAYING CYBER-SECURE THROUGH THE PANDEMIC

ALLIANZ RISK CONSULTING

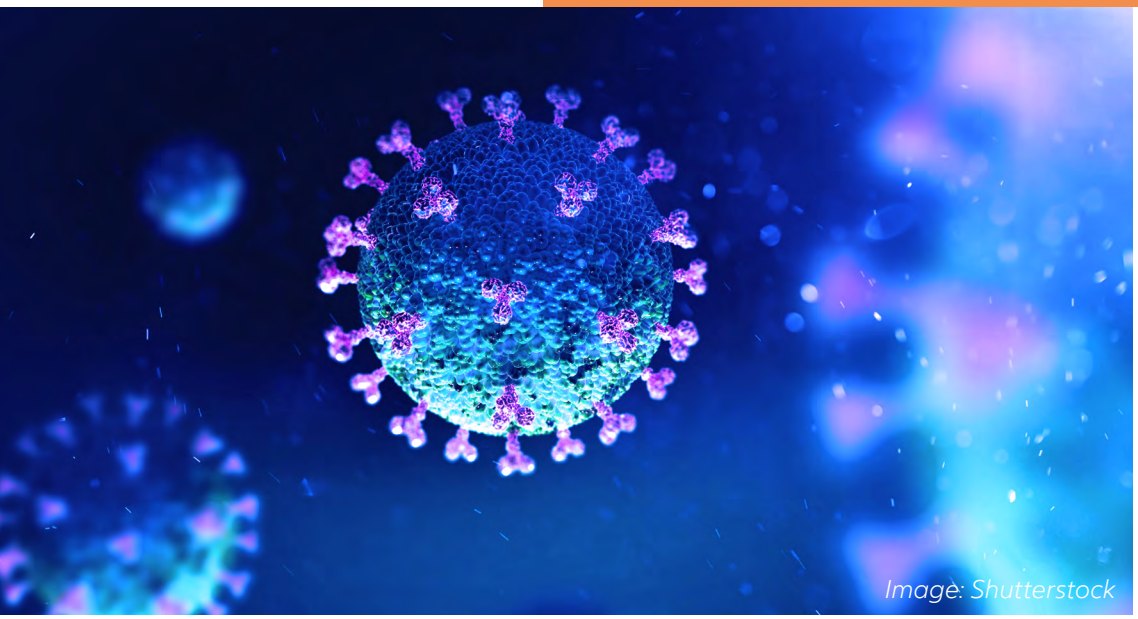

Image: Shutterstock

With many people working remotely because of the coronavirus outbreak, the number of cyber incidents is increasing as hackers, scammers and spammers look to exploit vulnerabilities in an attempt to steal valuable information. In response Allianz Global Corporate & Specialty (AGCS) experts highlight a number of measures that can help employees to better combat the cyber challenges Covid-19 brings.

Coronavirus is changing how people work and interact every day. Many companies have needed to expand their remote working capacity as a result of the outbreak – and usually at very short notice. In order to provide as many employees as possible with easy access to operating software and systems quickly, in some cases IT security standards may have had to be lowered or suspended, resulting in potential cyber security exposures for companies.

One consequence of potentially laxer security may be that cybercriminals and hackers may find it easier to penetrate previous effectively-protected corporate systems, causing data breaches, cyber blackmail intrusions and IT system failures. Unfortunately, the home worker accessing the corporate network with a virtual private network (VPN) connection is a desirable target for cyber criminals and recent events only demonstrate this.

Coronavirus phishing scams with malicious links or attachments sent out by email or WhatsApp messages started circulating in January 2020 and they've only proliferated since. The European Commission has said that cybercrime in the EU has increased since the outbreak began, while The World Health Organization (WHO) recently warned about suspicious email messages attempting to take advantage of the Covid-19 emergency[1] by stealing money and sensitive information from the public. In some countries, data shows that the number of attempted cyber attacks has increased five-fold between mid-February and mid-March.

[1]World Health Organization, Beware of criminals pretending to be WHO, 2020

Allianz

"Remote workers may be dressing down in the home office but this does not mean that they can be casual when it comes to maintaining IT security standards," says Jens Krickhahn, Practice Leader Cyber Insurance, AGCS Central and Eastern Europe.

For example, certain IT security standards are a prerequisite for a company to take out cyber insurance. For this reason, AGCS has prepared the following overview of tips and measures to consider to protect against internet attacks. These are based on the core measures of the German Federal Office for Information Security ("Bundesamt für Sicherheit und Informationstechnik") and the guidelines of the Charter of Trust, an association of companies promoting global IT security, of which Allianz is a member, and apply to all devices, including those provided by companies for employees to use. Any additional or deviating guidance of the respective local official body/administration prevails.

All of the recommendations are technical advisory in nature from a risk management perspective and may not apply to your specific operations. Please review recommendations carefully and determine how they can best apply to your specific needs prior to implementation. Any queries relating to insurance cover should be made with your local contact in underwriting, agent and/or broker.

CORE MEASURES FOR IT SECURITY IN THE HOME OFFICE

KEEP SOFTWARE UP-TO-DATE

Check whether you can use current versions of operating systems and installed programs. If possible, use the automatic update feature, which is often the default setting. Otherwise, immediately install security updates for your software, especially for your web browser and operating system.

USE VIRUS PROTECTION AND FIREWALLS

Check activation of virus protection and firewalls, but keep in mind that this measure can only be effective as an accompanying measure with other security procedures. Its application does not reduce the importance of the other tips mentioned here.

CREATE DIFFERENT USER ACCOUNTS

Malicious programs have the same rights on the PC as the user account through which they entered the computer. You should, therefore, only work with administrator rights if absolutely necessary.

BE CAUTIOUS ABOUT SHARING PERSONAL DATA

Online fraudsters increase their success rates by addressing their victims individually: Previously spied-on data, such as surfing habits or personal names, are used to inspire confidence. Today, personal data is considered a currency on the internet and is traded in this way. If possible, use a VPN connected to your home network in public wireless local area network (WLAN) hotspots. Otherwise, unencrypted transmitted data can be read by third parties. At the same time, a VPN also protects against a number of other attacks on the PC and the data stored on it.

ADDITIONAL MEASURES FOR IT SECURITY IN THE HOME OFFICE

ONLY TAKE HOME THOSE DEVICES AND INFORMATION THAT ARE ABSOLUTELY NECESSARY

The best way to protect information or devices from loss is not to remove them from your corporate environment in the first place. That way, they won't get lost in transit or at home. Only take home the devices and information you really need.

USE UP-TO-DATE WEB BROWSERS

Check whether to disable components and plug-ins in your browser settings. First, enter the addresses for particularly security-critical websites, such as for online banking, manually in the address line of the browser and save the address entered in this way as a bookmark, which you can then use for secure access.

REFRESH PASSWORDS OFTEN

Keep all passwords and user names safe and change any passwords that may have fallen into the wrong hands as quickly as possible. Use different, unrecognizable passwords for different applications and change the passwords preset by the manufacturers before first use. It is important that you can remember a password well. The general rule is: the longer, the better. The password should be at least eight characters long, should not appear in the dictionary and should consist of upper and lower case letters as well as special characters and numbers.

TWO-FACTOR AUTHENTICATION

Where two-factor authentication is offered, use it to secure access to your account. A password manager can facilitate the handling of different passwords. Do not share your passwords with third parties.

PROTECT YOUR DATA THROUGH ENCRYPTION

Protect your confidential emails with encryption. If a WLAN is used, subject to the information security guidance of your entity, pay attention to the encryption of the wireless network. Subject to higher standards as per individual guidance of the respective Individual Security Officer (ISO), in your router, select the WPA3 encryption standard or, if this is not yet supported, WPA2, until further notice. Choose a complex password of at least 20 characters.

ONLY DOWNLOAD DATA FROM TRUSTED SOURCES

Be careful when downloading something from the internet. Before downloading programs, make sure that the source is trustworthy. If possible, use the manufacturer's website to download them.

BACKUP DATA ON A REGULAR BASIS

If, despite all the protective measures, the PC is infected, important data can be lost. In order to minimize the damage, make regular backups of files, subject to local/individual ISO guidance.

TURN OFF VOICE-ACTIVATED SMART DEVICES IN THE HOME OFFICE AND COVER THE WEBCAM WHEN NOT IN USE

Voice assistants hear what is being said in the room and transmit it to the provider. There is no guarantee that these recordings will not fall into the wrong hands. And be sure to cover the PC's webcam when not in use and be careful what is exchanged via the video function.

DO NOT MIX PERSONAL AND BUSINESS USE

Make a clear distinction between devices and information for business and personal use and do not transfer work data to personal devices. This will prevent unintentional information leakage. As a side effect, it also helps to psychologically separate "work" time from "home" time.

IDENTIFY ALL PARTICIPANTS IN ONLINE SESSIONS

It is particularly easy for unauthorized persons who have obtained the dial-in data to join a large online meetings with many participants. That's why everyone who appears in the meeting needs to briefly identify themselves, especially when discussing sensitive topics and sharing presentations on screen.

LOG OUT WHEN DEVICES ARE NO LONGER IN USE AND KEEP THEM SAFE

Even if it's just a short break, lock the PC and mobile device screens, as if you were at work, so that they are not accessible to others. And, of course, protect the devices themselves against unauthorized use or even theft when they are at your home.

FOLLOW SECURITY PRACTICES FOR PRINTING AND HANDLING CONFIDENTIAL DOCUMENTS

Keep your desk free of confidential printouts. "Unauthorized use" can even include children using work papers as drawing paper. Lock confidential documents in a cabinet when you don't need them. Do not dispose of internal or confidential documents in your normal wastebasket: shred internal or confidential documents before disposing of them. If you do not have a shredder, collect all internal or confidential documents and check whether you can bring them back to the office for safe disposal when work from home is over.

BE EXTREMELY CAREFUL WITH SUSPICIOUS E-MAILS OR ATTACHMENTS, ESPECIALLY IF THE SENDER IS UNKNOWN

Especially in the familiar environment of your home office, you must be wary of suspicious e-mails. Take your time and check each email thoroughly before you open it.

FURTHER INFORMATION*

The guidelines of the Charter of Trust, an association of companies promoting global IT security

https://www.charteroftrust.com/

Specialist services to help identify companies' cyber risks

https://www.agcs.allianz.com/services/cyber-risk-management.html

CONTACTS

Rishi Baviskar
Cyber Experts Group Leader, Allianz Risk Consulting
rishi.baviskar@allianz.com

Jens Krickhahn
Practice Leader, Cyber Insurance, AGCS CEE
jens.krickhahn@allianz.com

Yogesh Virji
Head of Cyber Insurance, AGCS UK
yogi.virji@allianz.com

Design: Graphic Design Centre

Allianz Global Corporate & Specialty SE, Fritz-Schäffer-Strasse 9, 81737 Munich, Germany

Commercial Register: Munich, HRB 208312