

CYBER ADVENT CALENDAR

It's the most wonderful time of the year... also for cybercriminals!
Get to know the fraudsters' favorite tricks and stay one step ahead with these tips.

 <p>REPORT CYBERCRIME</p> <p>Stay alert and always report online crime. You may help prevent others from becoming victims.</p> <p>REPORT</p>	<p>BUY THE REAL DEAL</p> <p>Your loved ones deserve the best gifts. #DontFakeUp! Think twice before purchasing a seemingly too good to be true gift, it could be counterfeit!</p> 	 <p>SECURE PASSWORDS</p> <p>Passwords provide the first line of defence against unauthorized access to your electronic devices. The stronger your password, the more protected you will be.</p>
<p>PROTECT CHILDREN</p> <p>Talk to your child about cyber safety. Listen to their online experiences and explain to them the importance of being just as safe online as offline.</p> 	 <p>RISKS OF USING PUBLIC WI-FI</p> <p>Public Wi-Fi hotspots can provide an easy way for identity thieves and criminals to monitor what you are doing online.</p>	
 <p>NO MORE RANSOM</p> <p>Ransomware holds your data hostage for a price. You can infect your devices visiting compromised websites, clicking on malicious attachments or downloading compromised software.</p>	<p>KNOW YOUR FINANCES</p> <p>Check your bank statement regularly. Notify your bank immediately if you see payments or withdrawals that you have not made yourself.</p> 	<p>CONNECTED TOYS</p> <p>Internet-enabled devices help to educate children through interactive play. Make sure you get to know its security settings & set up parental controls.</p> 
	<p>CEO/ BEC FRAUD</p> <p>Criminals try to take advantage of employees authorised to make payments and trick them into paying a fake invoice or making an unauthorised transfer out of the business account.</p> 	<p>MOBILE MALWARE</p> <p>Before downloading an app, research the app and its publishers. Check other users' reviews and the app permissions. Just because an app is in the official App Store it doesn't mean it's legitimate!</p> 
 <p>VISHING</p> <p>A combination of the words <i>Voice</i> and <i>Phishing</i>, it's a phone scam in which fraudsters try to trick you into divulging personal, financial or security information or into transferring money to them.</p>	<p>SELL SAFE</p> <p>How safe is your online shop? Consider the cybersecurity dimensions:</p> <ol style="list-style-type: none">1) prepare your business2) set your defences3) sell & get paid safely4) reach out if you need help. <p>#Sellsafe</p> 	<p>KEEP CALM AND BACK UP!</p> <p>Regularly back up data stored on your electronic devices. Keep at least one copy offline. Backing up your data can give you the upper hand in case of a ransomware attack.</p> 
	 <p>YOUR LIFE IS ONLINE, PROTECT IT</p> <p>Your digital life needs as much protection as your home. Avoid announcing the dates of your trips or your current location on social media.</p>	 <p>MERRY CHRISTMAS!</p>
 <p>FAKE TRAVEL DEALS</p> <p>From fraudulent flights to non-existing accommodation, holiday fraud is a big business for scammers and is most frequent during peak holiday times.</p>	 <p>BUY SAFE PAY SAFE</p> <p>When shopping online: buy from trusted sources, stay alert for #2good2btrue offers and keep all relevant emails following the purchase.</p>	 <p>PAY SAFE... ONLINE & OFFLINE</p> <p>When using a card to pay in a retail outlet:</p> <ol style="list-style-type: none">1) cover your PIN2) check the total amount before paying3) never lose sight of your card4) save the transaction receipts.
<p>FAKE DELIVERY MESSAGES</p> <p>Watch out for unexpected and vague notifications claiming to be related to a delivery. They can be leading you to malicious websites.</p> 	<p>SAFE TELEWORKING</p> <p>If you are working remotely, maintain an adequate level of cybersecurity.</p> 	
 <p>WHAT'S IN THE BOX?</p> <p>Fraudsters can use fake job offers to trick you into reshipping illegally obtained items. If you are offered money to receive a package and send it to someone else, you are being asked to be a parcel mule.</p>	<p>WHO ARE YOU TALKING TO?</p> <p>People can easily lie about who they are online and pretend to be someone they are not, including a friend, a mentor or a boyfriend/ girlfriend. Always take your time and do your research.</p> 	<p>FAKE CHARITIES</p> <p>Always double check the authenticity of a charity before providing financial details and donating money. If you have provided your account details to a fraudster, contact your bank & report it to the police.</p> 
	 <p>STAY UP TO DATE</p> <p>Software and operating system updates address security vulnerabilities and fix bugs. The sooner you install them the less vulnerable your device is to criminals.</p>	 <p>INVESTMENT FRAUD</p> <p>Common investment scams may include lucrative investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy.</p>