Digitale Oasen entdeckt

Wie sicher bewegen wir uns (gefühlt) im vernetzten zu Hause seit Corona?

kaspersky BRING ON THE FUTURE

Inhalt

Methodik	3
Haupterkenntnisse der Studie aus den digitalen Oasen der DACH-Region	4
Haupterkenntnisse der Studie aus den digitalen Familien-Oasen weltweit	5
The New Normal	6
Digitale Oasen seit Corona	7
Wie gefährlich sind Video-Streams und Online Games?	9
Wie cybersicher bewegen wir uns in der digitalen Oase?	11
Gefühlte Sicherheit: Bei mir gibt es nichts zu holen!	12
Digitale Oasen werden zum Mittelpunkt des Familienlebens	13
Online-Überweisungen lieber im Büro erledigt	14
Eltern verbringen mehr Zeit online als der Durchschnitt	15
Wer übernimmt die Führungsrolle in Sachen Technologie zu Hause	16
Cybersicherheit für die ganze Familie	17
Wie man seine digitale Oase vor unerwünschtem Zugriff schützt	18

Methodik

In einer von Kaspersky beauftragten, internationalen Umfrage von SAPIO Research wurden im Mai 2020 weltweit mehr als 10.000 Nutzer online befragt, die mindestens zwei im Haushalt vernetzte Geräte nutzen. Im deutschsprachigen Raum (DACH-Region) wurden 1.010 Nutzer befragt – 506 Deutsche, 251 Österreicher und 253 Schweizer.

Forciert durch Corona haben sich zu Hause virtuelle Wohlfühlecken herausgebildet. Diese digitalen Oasen etablieren sich nun immer stärker als wichtiger Bestandteil des Lebens.

Haupterkenntnisse der Studie aus den digitalen Oasen der DACH-Region

Das Internet wurde zu Hause während Corona intensiv genutzt und damit ist die verbrachte Zeit bei fast der Hälfte der Befragten (45 Prozent) in Deutschland, Österreich und der Schweiz um mindestens zwei Stunden pro Tag gestiegen: Dabei haben Nutzer ihre Onlinezeit mit E-Mails (70 Prozent), Online-Shopping (60 Prozent), Social Media (59 Prozent), Online-Banking (58 Prozent) und dem Lesen von News (56 Prozent) verbracht. Gefolgt vom Streamen von Filmen und Serien (49 Prozent), Musik (42 Prozent) sowie Online-Gaming (40 Prozent).

Trügerische IT-Sicherheit in den eigenen vier Wänden: Trotz erhöhter Internetnutzung denkt mehr als jeder Dritte (37 Prozent), er sei kein lohnenswertes Ziel für Cyberkriminelle.

Erhöhtes Cyberrisiko durch verstärktes Online-Shopping und Online-Banking? Die befragten Nutzer haben mehrheitlich (75 Prozent) private Tätigkeiten aus dem realen ins virtuelle Leben übertragen. Neben dem Kontakt mit Freunden und Familie (45 Prozent) zieht ein Viertel (23 Prozent) jetzt aufgrund von Corona Online-Banking dem Besuch in einer Filiale vor, außerdem shoppt ein Drittel (36 Prozent) nun lieber im Web als im Geschäft vor Ort.

Finanz- und Bezahldaten sind (derzeit) ein besonders wertvolles Gut im Cyberuntergrund. Die Kaspersky-Analysen zeigen: Mehr als die Hälfte aller Phishing-Angriffe hat Finanz- und Bezahldaten im Visier (egal ob Windows oder Mac). Bereits im vergangenen Jahr gab es eine Verdreifachung im Bereich Banking-Malware. Werden jetzt mehr Transaktionen über das Internet getätigt, ist besondere Vorsicht angesagt.

Das Cyberrisikopotential von Gaming und Streaming wird unterschätzt. Die Hälfte der Befragten sagt, dass sie aufgrund erhöhter Web-Aktivität bei Online-Datings (49 Prozent) und virtuellen Meetings (36 Prozent) sowie Online-Finanzangelegenheiten (48 Prozent) die meisten Sicherheitsbedenken hatten. Der Bereich Online-Entertainment wird hier mit 29 Prozent als weit weniger bedenklich erachtet. Auch hier zeigt sich, dass die gefühlte Sicherheit der Befragten nicht mit der IT-Sicherheitsforschung übereinstimmt. Das bestätigen die Beispiele Video-Streaming und Online-Gaming:

- So ging weltweit mehr als jede zehnte im Zusammenhang mit Netflix stehende Attacke auf das Konto von Nutzern in Deutschland.
- Auch stiegen während der Corona-bedingten Ausgangsbeschränkungen weltweit die Angriffe unter dem Deckmantel beliebter Online-Spiele oder Plattformen wie beispielsweise Minecraft oder Counterstrike um mehr als 50 Prozent an.

Die Ergebnisse beziehen sich auf 1.010 befragte Nutzer aus der DACH-Region: 506 Deutsche, 251 Österreicher und 253 Schweizer.

Haupterkenntnisse der Studie aus den digitalen Familien-Oasen weltweit

Account-Sharing beliebt: Fast die Hälfte (46 Prozent) der Befragten loggt sich mit einem Passwort in Streaming-Accounts wie Netflix oder Apple TV mit Mitbewohnern, Familie oder Freunden ein.

Eltern verbringen mehr Zeit online als der Durchschnitt: Im Durchschnitt verbringen die befragten Väter und Mütter sieben Stunden und zwölf Minuten pro Tag online, fast eineinhalb Stunden mehr als der Durchschnitt der Umfrageteilnehmer.

Mehr Gefahren durch Homeoffice? Nachdem das Arbeitsleben zu Hause Einzug hielt, sind 67 Prozent der Eltern insbesondere über die Risiken ihrer verstärkten Online-Aktivitäten im Umgang mit finanziellen Angelegenheiten besorgt.

Wer hat die IT-Hosen an? Väter (82 Prozent) wie Mütter (61 Prozent) behaupten von sich, die Entscheidungen über Technologie innerhalb der Familie zu treffen.

Großes Vertrauen bei der Online-Nutzung der Kinder: Ein Drittel (33 Prozent) der befragten Eltern ist in jüngster Zeit nachsichtiger geworden in Bezug auf die Zeit, die ihre Kinder online verbringen. Dennoch machen sich 29 Prozent um die Sicherheit ihrer Kinder Sorgen. Mehr als die Hälfte (52 Prozent) der Familien vertraut ihren Kindern, dass sie sich online selbst zu schützen wissen.

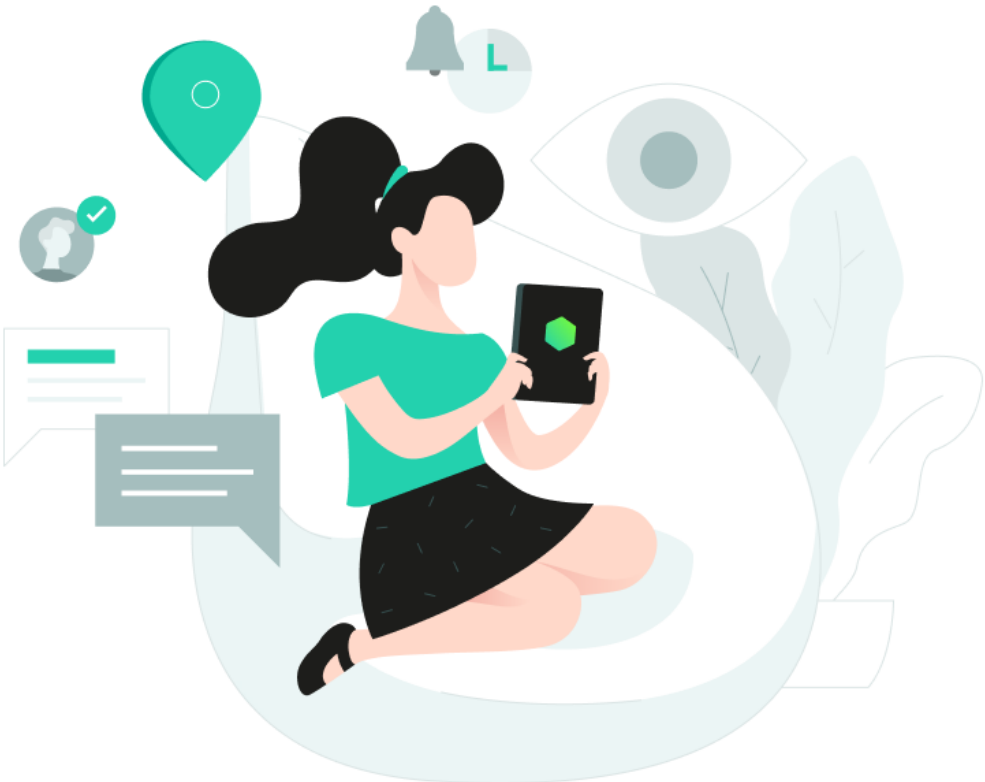
Die Ergebnisse beziehen sich auf 3.834 internationale Nutzer mit Kindern, die innerhalb der Kaspersky-Studie befragt wurden.

The New Normal

Als die Politik in den meisten Ländern Mitte März dieses Jahres Ausgangsbeschränkungen beschloss, haben wir so viel Zeit wie wahrscheinlich selten zuvor zu Hause verbracht. Ob Arbeit, Familienleben oder Freizeitgestaltung – unser Leben spielte sich in den vergangenen fünf Monaten verstärkt in den eigenen vier Wänden ab.

Die Bedeutung von Technologie in der eigenen Wohnung war größer als je zuvor. Internet, Smartphone, Computer und Spielkonsole waren essenziell für den Alltag, für Homeschooling und zur Unterhaltung. Wir haben es uns digital „eingerichtet" und „bequem" gemacht, es sind (neue) digitale Oasen entstanden, in denen unser Cyberleben intensiver stattfindet als zuvor. Doch wie hat sich unser Nutzungsverhalten wirklich verändert? Fühlen wir uns dabei sicher? Und was sagen die Experten im Hinblick auf potentielle Cyberrisiken im vernetzen Home-sweet-Home?

Eine groß angelegte internationale Studie von Kaspersky, bei der auch über eintausend deutsche, österreichische und Schweizer Verbraucher im Mai 2020 befragt wurden, zeigt unser (neues) digitales Nutzungsverhalten und wie cybersicher wir uns in den eigenen vier Wänden bewegen. Besonders spannend: Das vorherrschende Sicherheitsgefühl bei den Deutschen, Österreichern und Schweizern wird mit den aktuellen Erkenntnissen aus der Forschungs- und Analyse-Abteilung von Kaspersky abgeglichen. Denn eines ist klar: Vermehrtes Streaming, Gaming, Shopping und Banking rufen auch das Interesse von Außenstehenden, von Cyberkriminellen hervor.



Digitale Oasen seit Corona

Das Internet spielt zu Hause eine zentrale Rolle. Durch die Corona-Pandemie haben sich zudem viele Dinge, die man vormalig im realen Leben gemacht hat, ins Web verlagert. Die Umfrage von Kaspersky bestätigt das. Demnach haben die Nutzer mehrheitlich (75 Prozent) ihre privaten Tätigkeiten aus der Realität ins Internet verlegt. Neben Socialising mit Freunden und Familie (45 Prozent) ziehen laut Umfrage 23 Prozent der im DACH-Raum Befragten Online-Banking dem Besuch einer Filiale vor, außerdem shoppen 36 Prozent lieber im Web als im Geschäft vor Ort.

Doch wie sicher fühlen sich die Nutzer in Deutschland, Österreich und der Schweiz dabei, wenn sie vermehrt auch sensible Transkationen wie Shopping und Banking zu Hause durchführen? Laut der Kaspersky-Umfrage sorgen sich die Befragten in der DACH-Region generell weniger (29 Prozent) um die Sicherheit des Internets zu Hause als im internationalen Vergleich (48 Prozent). Die Sorge steigt, wenn es um kritische Bereiche und wertvolle Daten geht. Das sagen 66 Prozent der DACH-Befragten (weltweit 77 Prozent). Sie sorgen sich im Speziellen vor Spionage (43 Prozent), Tracking (42 Prozent) oder dem Zugriff von Dritten auf Finanz- und Zahlungsinformationen (44 Prozent).

Insgesamt bestätigt die Hälfte (48 Prozent) der Befragten, dass sie aufgrund erhöhter Web-Aktivität im Corona-Lockdown die größten Sicherheitsbedenken bei Online-Datings (49 Prozent) und virtuellen Meetings (36 Prozent) sowie Online-Finanzangelegenheiten (48 Prozent) haben.

Das Bewusstsein für IT-Sicherheit und Datenschutz ist also vorhanden, allerdings geringer als im internationalen Vergleich. Muss man heute eher vom „German Leichtsinn" als von der „German Angst" sprechen? Zieht man die Analysen der Sicherheitsforscher zu Rate, könnte man diese etwas überspitzte These mit „Ja" beantworten.

So zeigte eine Langzeitanalyse von Kaspersky unlängst, dass bereits im vergangenen Jahr Nutzer in Deutschland (21 Prozent aller Attacken weltweit) fast dreimal so häufig wie im Jahr 2018 (7 Prozent aller Attacken weltweit) von Banking-Malware attackiert wurden. Sieht man sich die User an, die von Phishing-Angriffen besonders betroffen waren, stellt man fest, dass im vergangenen Jahr

- 27 Prozent (Mac-Nutzer: 36 Prozent) aller Angriffe gegen Online-Banking-Nutzer
- 17 Prozent (Mac-Nutzer: 10 Prozent) gegen E-Paymentsystem-Nutzer
- und 8 Prozent gegen Online-Shopper (Mac-Nutzer: 9 Prozent) gerichtet waren.

Das heißt: Die Mehrheit der Phishing-Angriffe gegen Computernutzer – nämlich 52 Prozent (im Mac-Bereich sogar 55 Prozent) – hat es auf Finanzangelegenheiten abgesehen.

Phishing ist für Cyberkriminelle eines der Standbeine schlechthin – technisch einfach in der Durchführung, massenhafte Verbreitung und damit hohe Erfolgsaussichten; und – besonders prekär und anders als bei Schadsoftware – unabhängig vom eingesetzten Betriebssystem. Es spielt kaum eine Rolle, ob das potentielle Opfer die E-Mail zuerst auf dem Smartphone, Tablet, einem Mac, Linux oder Windows System abruft.

Christian Funk, Leiter des Forschungs- und Analyse-Teams DACH bei Kaspersky

Wie gefährlich sind Video-Streams und Online Games?

Laut der Kaspersky-Studie nutzen 58 Prozent Video-Streaming auf ihren Geräten zu Hause. 49 Prozent bestätigen: Zum Zeitpunkt der Umfrage (Mai 2020) verbrachten sie ihre Online-Zeit häufig mit dem Schauen von Filmen und Serien. Eine aktuelle Analyse von Kaspersky zum Thema, wie Cyberkriminelle bösartige Dateien unter dem Namen beliebter Video-Streaming-Plattformen und deren Inhalten tarnen, zeigt:

Nutzer sollten sich von illegalen Inhalten fernhalten: So waren im Untersuchungszeitraum (Januar 2019 bis April 2020) mehr als 5.000 Nutzer unterschiedlichen Bedrohungen ausgesetzt, die versuchten, auf Netflix über inoffizielle Dateien mit dem Namen des Streaming-Dienstes zuzugreifen.

Deutsche Nutzer als beliebtes Ziel: Die meisten mit Netflix in Verbindung stehende Angriffe (Anteil weltweit: 11 Prozent) richteten sich gegen deutsche Nutzer. Dies hat vielfältige Gründe, beispielsweise dass Netflix in Deutschland sehr beliebt ist.

Nutzer aller großen Plattformen sollten Vorsicht walten lassen: Insgesamt konnten weltweit mehr als 22.000 Infektionsversuche identifiziert werden, die den Namen eines beliebten Streaming-Dienstes wie Disney +, Netflix, Apple TV Plus oder Amazon Prime Video als Lockmittel nutzten.

Vorsicht vor Phishing-Angriffen: Accountzugangsdaten der Nutzer von Video-Stream-Plattformen sind beliebt – auch hier stehen insbesondere Finanzinformationen wie Kreditkartendaten im Visier.

Die sogenannten ‚Streaming Wars' haben gerade erst begonnen und mit der wachsenden Beliebtheit der Plattformen wird auch die Aufmerksamkeit, die sie von Cyberkriminellen erhalten, größer. Dies gilt vor allem deshalb, weil viele der Plattformen ein beispielloses Wachstum erfahren, da zahlreiche Angestellte derzeit vermehrt von zu Hause aus arbeiten. Auch wenn Nutzer versucht sein mögen, nach alternativen Methoden zu suchen, um ihre Lieblingsinhalte online zu sehen, anstatt für ein weiteres, sicheres Abonnement zu bezahlen, ist die beste Option immer noch der Zugang zu Plattformen und Angeboten offizieller Quellen.

Christian Funk, Leiter des Forschungs- und Analyse-Teams DACH bei Kaspersky

Zur Unterhaltung (58 Prozent) werden in der DACH-Region Geräte zu Hause auch für Online-Games gerne genutzt. Auch ist bei über der Hälfte (53 Prozent) der Befragten eine Spielkonsole aktiv. Analysen von Kaspersky zeigen: Für Gamer stieg – vor allem Corona-bedingt – das Cyberrisiko. Demnach gab es während der Ausgangsbeschränkungen weltweit einen Anstieg um 54 Prozent von Angriffen unter dem Deckmantel beliebter Spiele oder Plattformen wie beispielsweise Minecraft oder Counterstrike. Darüber hinaus fanden die Experten von Kaspersky vier Malware-Familien, die explizit Passwörter und Daten von Gamern im Blick haben und entwenden können. Daher sollte man beim Gaming – wie beim Shopping, Banking und Streaming – besonderes Augenmerk auf die eigenen Kontodaten haben.

Viele dieser Angriffe im Zusammenhang mit Videospielen sind nicht besonders ausgefeilt. Der Nutzer als Angriffsvektor führt hier zum Erfolg. Die vergangenen Monate haben gezeigt, dass Nutzer sehr anfällig für Phishing-Angriffe oder das Klicken auf schädliche Links sind, wenn sie auf der Suche nach Raubkopien oder Cheats sind, die ihnen beim Weiterkommen in den Spielen helfen.

Da nun viele Spieler dieselben Geräte zum Gaming verwenden, mit denen sie auch auf Unternehmensnetzwerke zugreifen, sollten sie erst recht Vorsicht walten lassen: Riskante Aktionen gefährden nicht nur persönliche Daten oder Geld, sondern auch Unternehmensressourcen. Wenn möglich, sollten Nutzer vermeiden, ihre privaten Geräte für Unternehmenszwecke einzusetzen und umgekehrt.

Christian Funk, Leiter des Forschungs- und Analyse-Teams DACH bei Kaspersky

Wie cybersicher bewegen wir uns in der digitalen Oase?

Wenn man davon ausgeht, dass Cyberkriminelle insbesondere Account-Zugänge und Finanz- und Zahlungsdaten wie Kreditkartendaten im Visier haben, stellt sich die Frage: Wie gut sind das Internet und die damit verbundenen Geräte abgesichert?

Laut der aktuellen Befragung von Kaspersky führt die Hälfte (52 Prozent) der Nutzer in Deutschland, Österreich und der Schweiz regelmäßig Anti-Viren-Scans auf ihren Geräten durch. Lediglich 44 Prozent beziehen ausschließlich Apps aus offiziellen Quellen wie Google Play oder dem App Store. 41 Prozent ändern regelmäßige ihre Passwörter – was nicht unbedingt empfohlen wird – und nutzen einzigartige Passwörter – ein absolutes Muss, am besten mit 16 Stellen inklusive Sonderzeichen und Ziffern. Warum dies so wichtig ist, erklären die Kaspersky-Experten in folgendem Video: https://www.youtube.com/watch?v=sxR2lvUq1YA

Interessant: Während 82 Prozent der Meinung sind, dass Smartphones mit Passwörtern geschützt sein sollten (bei Computern: 81 Prozent), stimmen nur 62 Prozent der Aussage zu, dass das eigene WLAN passwortgeschützt sein sollte. Geht es um die WLANs der Nachbarn, zeigt sich ebenfalls ein interessantes Bild:

- 43 Prozent haben vom Netzwerk der Nachbarn nie etwas mitbekommen;
- neun Prozent sagen jedoch, sie könnten sich damit verbinden, und acht Prozent haben sich tatsächlich schon einmal heimlich dort eingewählt.
- weitere 11 Prozent hegen die Befürchtung, dass die Nachbarn sich in ihr eigenes WLAN einwählen, ohne eine vorige Erlaubnis eingeholt zu haben.

Ein ordentliches und konsequentes Passwortmanagement ist für Internetnutzer Pflicht, da dies unser Tor zu fast sämtlichen Diensten darstellt. Bei oftmals Dutzenden solcher Dienste hilft ein Passwort-Manager, der dem Nutzer im Dschungel der Zugangsdaten unter die Arme greift. Vermehrt bieten Portale auch Zwei-Faktor-Authentifizierung an, was vor allem bei subjektiv kritischen Resourcen sehr zu empfehlen ist. Dies steigert die Zugangssicherheit enorm.

Unser Zuhause ist stärker vernetzt als je zuvor. Wir nutzen mehr und mehr neue Technologien, um unser Leben komfortabler zu gestalten. Da die Nachfrage nach Smart-Home-Geräten steigt, sind sie attraktive Ziele für Cyberkriminelle. Was kann passieren, wenn in unser smartes Zuhause eingebrochen wird? Cyberkriminelle könnten die Kontrolle über alle intelligenten Geräte und Anwendungen erlangen, die mit dem Heimnetzwerk verbunden sind, was einige unangenehme Folgen haben kann. Daher ist es wichtig zu wissen, wie man diese Geräte schützt: Vor dem Kauf sollte man Rezensionen und Studien über die Sicherheit der Geräte lesen. Nachdem man sich für eine bestimmte App oder ein bestimmtes Gerät entschieden hat, sollte man sich über Updates und entdeckte Schwachstellen auf dem Laufenden halten; Geräte und Bedienfelder mit einem starken, eindeutigen Kennwort schützen und das WLAN-Heimnetzwerk korrekt konfigurieren.

Christian Funk, Leiter des Forschungs- und Analyse-Teams DACH bei Kaspersky

Gefühlte Sicherheit: Bei mir gibt es nichts zu holen!

Die Mehrheit (57 Prozent) der Deutschen, Österreicher und Schweizer behauptet, dass sie bisher noch nicht gehackt wurden. Hingegen haben 43 Prozent bereits Erfahrung mit Hacks gegen Social-Media- und sonstige Web-Konten, Computer, Smartphones oder andere Geräte im Eigenheim gemacht.

Mehr als jeder Dritte (37 Prozent) ist der Meinung, kein lohnenswertes Ziel für Cyberkriminelle zu sein, und jeder Vierte in DACH (24 Prozent) gibt zu, dass Internetsicherheit für ihn wichtig sei, allerdings häufig aufgrund anderer Prioritäten vernachlässigt werde. Die Nutzer im deutschsprachigen Raum tätigen im Übrigen doppelt so häufig diese Aussage (22 anstatt 11 Prozent) als der weltweite Durchschnitt, dass sie sich im Umgang mit Technologie nicht wohl fühlen, aber dennoch der Meinung sind, einigermaßen klarzukommen.

Danach befragt, was Nutzern in der DACH-Region eine „digitale Oase" bedeutet, antworteten 34 Prozent (weltweit 42 Prozent), dass sie sich sicher online bewegen können, ohne sich Sorgen um die Sicherheit und den Datenschutz machen zu müssen. Danach folgt „Technologie, die funktioniert und einfach zu bedienen ist" mit 21 Prozent (weltweit 18 Prozent).

Die Tatsache, dass Menschen heute mehr denn je miteinander verbunden sind, verbessert und bereichert unser Leben in vielerlei Hinsicht – von der Stärkung von Familienbanden und Freundschaften bis hin zu einer höheren Produktivität bei der Arbeit und der Vereinfachung von Offline-Aktivitäten, die nun virtuell stattfinden. Es stimmt, dass Technologie eine gewisse Besorgnis auslösen kann, deren Bewältigung Zeit und Mühe kostet, aber mittel- bis langfristig wird sie sich definitiv positiv auf unser psychologisches Wohlbefinden auswirken. Es hat keinen Sinn, neue Technologien als eine Gefahr zu sehen; sie sollten als eine Chance verstanden werden, unser tägliches Leben und unsere Beziehungen zu verbessern. Sicherheitsbedenken kann man durch spezielle Software entsprechend adressieren und durch eine offene Kommunikationskultur zwischen den beteiligten Personen thematisieren, das schließt Familienmitglieder, Mitbewohner und Kollegen ein. Neue Technologien eröffnen eine Vielzahl an Möglichkeiten, die positive Veränderungen aus beruflicher, persönlicher und sozialer Perspektive fördern; es ist nur eine Frage der Anpassung, unsere digitalen Oasen zu entdecken.

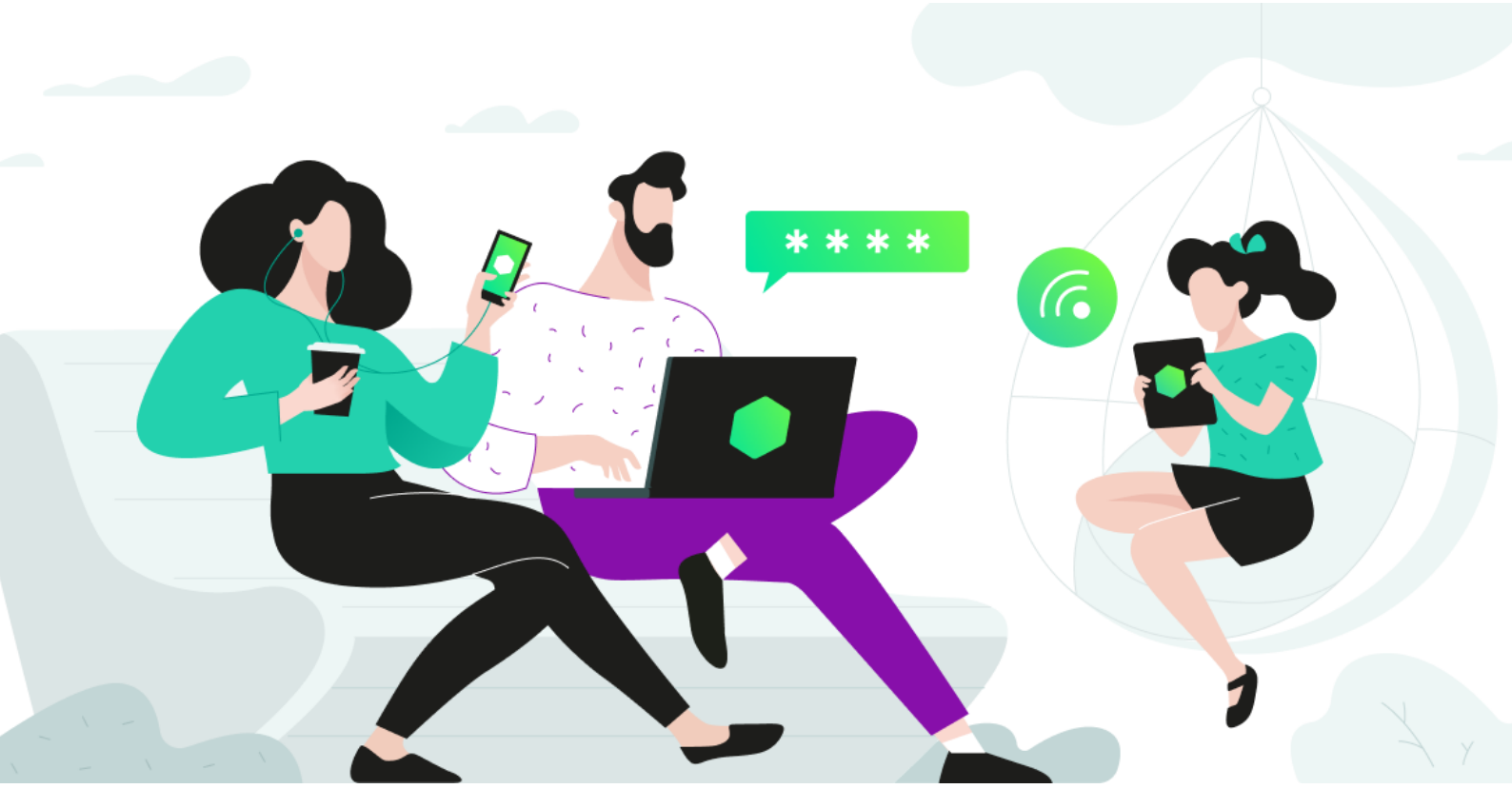
Dr. Berta Aznar Martínez, FPCEE Blanquerna – Ramon Llull University in

Digitale Oasen werden zum Mittelpunkt des Familienlebens

Digitale Oasen im eigenen Zuhause könnten sich zu einem wichtigen Bestandteil des allgemeinen Familienlebens entwickeln. Wer das Abendessen zusammen genießt, wird auch den gemeinsam gebuchten Streaming-Service nutzen – ob allein oder mit anderen vor dem Smart-TV.

Doch wer trifft hier die IT-Entscheidungen? Wer denkt an IT-Sicherheit und Datenschutz? Wie sehr vertrauen Eltern ihren Kindern, wenn diese verstärkt im Internet unterwegs sind? Die Studie von Kaspersky gibt auch hier interessante und zukunftsweisende Antworten. Die folgenden Zahlen beziehen sich allerdings im Vergleich zum ersten Teil des Berichts auf die internationalen Ergebnisse, da die Grundgesamtheit der Eltern mit Kindern, die in der Region DACH von Kaspersky befragt wurden, zu gering und damit zu wenig aussagekräftig ist, um lokale Schlüsse zu ziehen. Die folgenden Ergebnisse beziehen sich auf die weltweite Befragung von 3.834 Nutzern mit Kindern.

Das interessanteste Ergebnis vorweg: 46 Prozent teilen sich einen Streaming-Account wie Netflix oder Apple TV mit Mitbewohnern, Familie oder Freunden.

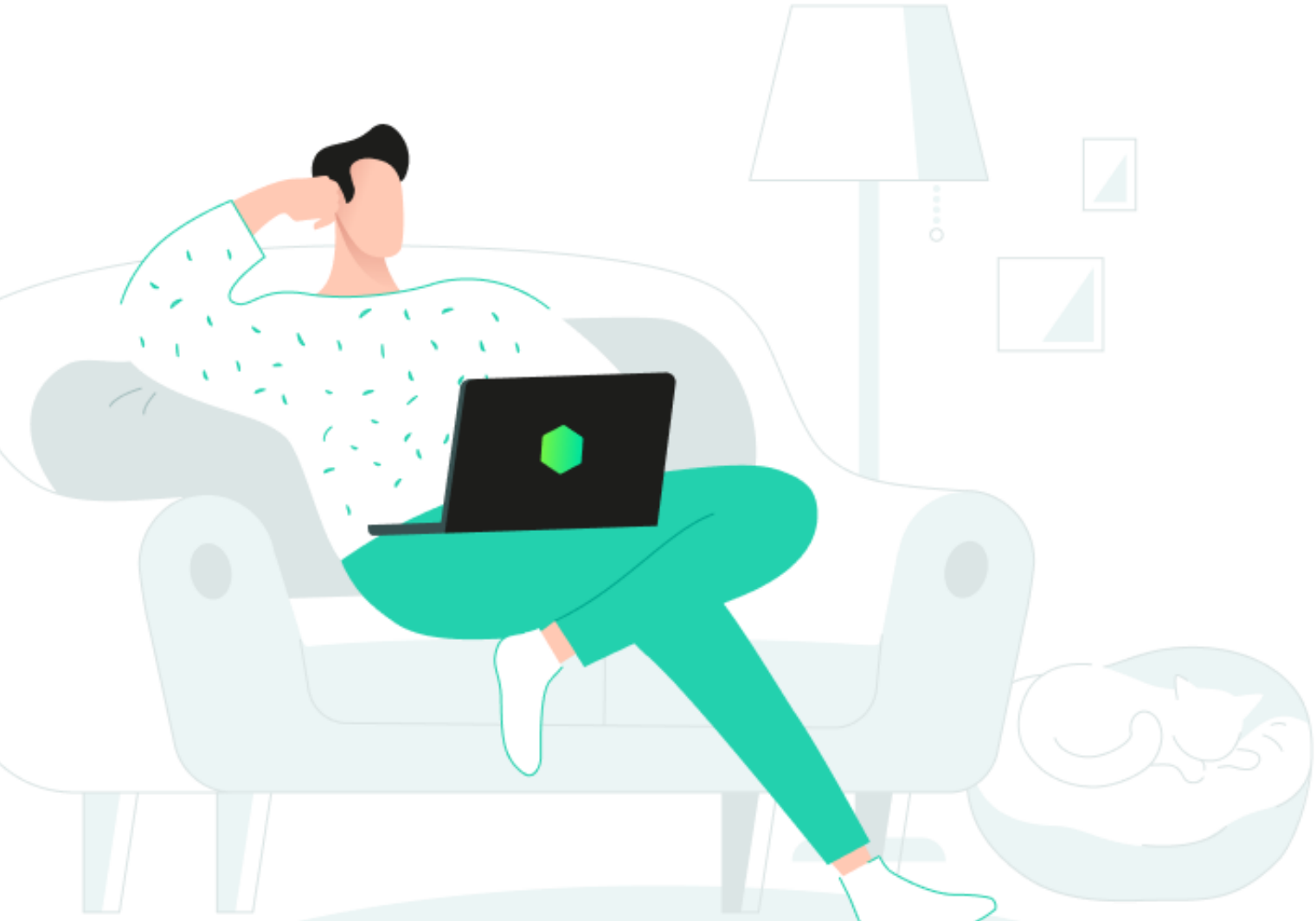


Online-Überweisungen wurden wohl früher lieber im Büro erledigt

Nachdem das Arbeitsleben zu Hause Einzug hielt, sind 67 Prozent der Eltern insbesondere über die Risiken ihrer verstärkten Online-Aktivitäten im Umgang mit finanziellen Angelegenheiten besorgt. Da es jetzt keine andere Möglichkeit gibt, als Online-Banking zu Hause zu erledigen, fühlen sich einige offensichtlich digital anfälliger, da sie zum Teil ihre eigenen Geräte benutzen müssen, mit denen sie sich weniger geschützt fühlen. Dies führt dazu, dass 67 Prozent dieser Eltern sich auch besorgt darüber äußern, dass jemand über ihre Geräte Zugang zu ihren Finanz- beziehungsweise Zahlungsdaten haben könnte.

Eltern verbringen mehr Zeit online als der Durchschnitt

Im Durchschnitt verbringen die befragten Väter und Mütter sieben Stunden und zwölf Minuten pro Tag online, was fast eineinhalb Stunden mehr ist als der Durchschnitt in der Umfrage. Das spiegelt höchstwahrscheinlich den Bedarf an Homeschooling und Unterhaltung der Kinder wider. Darüber hinaus ist ein Drittel (33 Prozent) der befragten Eltern in jüngster Zeit nachsichtiger geworden in Bezug auf die Zeit, die ihre Kinder online verbringen. Durch den Lockdown mussten Eltern, die im Homeoffice arbeiten, Online-Aktivitäten nutzen, um ihre Kinder während des Arbeitstages zu unterhalten, da sie nicht so viel nach draußen gehen konnten.



Wer übernimmt die Führungsrolle in Sachen Technologie zu Hause?

Die Ergebnisse zeigen auch interessante Widersprüche auf. Vier Fünftel der Väter geben an, dass sie bei IT-Entscheidungen für ihren Haushalt die Führung übernehmen. Dem widersprechen jedoch fast drei Fünftel der Mütter, die angeben, dass sie in Wirklichkeit diese Rolle wahrnehmen, angesichts ihres hohen Vertrauens in ihre technologischen Fähigkeiten. Diese Zahlen zeigen, dass sowohl Männer als auch Frauen der Meinung sind, dass sie in ihrer Beziehung die „digitalen Hosen anhaben".

Cybersicherheit für die ganze Familie

Speziell auf die Sicherheit der Kinder im Internet bezogen, sind 19 Prozent der Familien der Meinung, dass alle Geräte gut geschützt sind. Da jedoch 45 Prozent der Eltern glauben, dass ihre Kinder im vergangenen Jahr mehr Zeit online verbracht haben, machen sich 29 Prozent um die Sicherheit ihrer Kinder Sorgen. Es besteht offenbar ein Gefühl der Unsicherheit bei Eltern, die versuchen, das Online-Verhalten ihrer Kinder zu überwachen. Die Studie ergab, dass 73 Prozent der Eltern sich zumindest einigermaßen wohl fühlen mit der zusätzlichen Zeit, die ihre Kinder online verbringen; allerdings sind 35 Prozent auch der Meinung, dass man nie ganz gewiss sein kann, dass Kinder online sicher unterwegs sind.

Eltern sollten das Online-Verhalten in ihrer Familie genau kennen. Nur so können sie sich ein Bild der digitalen Spuren machen, die sie im Internet hinterlassen. Darauf basierend können sie – am besten zusammen mit ihren Kids – Regeln für die familiäre Internetnutzung aufstellen. Laut der Kaspersky-Studie haben 60 Prozent der befragten Eltern sehr strenge Regeln für ihre Kinder aufgestellt, um sie online zu schützen – zum Beispiel durch Begrenzung der Bildschirmzeit, das Einrichten von Kindersicherungstools oder das Verbot, dass die Kids unbegleitet surfen.

> Viele Familien durchlaufen große Veränderungen in ihrer Entwicklung aufgrund der zunehmenden Präsenz von Technologie in ihrem Leben. Diese neue Dimension prägt Familienbeziehungen und erfordert Umstellungen. Eltern sorgen sich darüber, dass ihre Kinder zu viel Zeit online verbringen und versuchen, eine Balance zwischen Online- und Offline-Zeit zu finden. Vor allem während der Ausgangsbeschränkungen befürchteten Eltern, dass ihren Kindern andere Aktivitäten fehlen, die gut für ihre Entwicklung und ihr Wohlbefinden sind, wie mit anderen Kindern zu spielen oder Sport zu treiben. Eltern befürchten auch, dass ihre Kinder von den neuen Technologien abhängig werden. Dazu kommen zudem Sorgen im Zusammenhang mit der Nutzung sozialer Netzwerke oder dem Zugang von Kindern zu digitalen Bereichen, die für sie nicht geeignet sind. Neben dem Komfort, den eine Sicherheitssoftware Eltern in diesen Fragen bietet, sollten sie mit ihren Kindern über mögliche Cybergefahren sprechen und gemeinsam Vereinbarungen treffen. Alle Familienmitglieder können davon profitieren, offen über diese Probleme zu reden und dadurch die Beziehung zueinander stärken.
>
> Dr. Berta Aznar Martínez, FPCEE Blanquerna – Ramon Llull University in Barcelona:

Da Kinder heute mit Technologie um sich herum aufwachsen, haben Eltern oft das Gefühl, selbst weniger Bescheid zu wissen – mehr als die Hälfte (52 Prozent) der Familien vertrauen ihren Kindern, dass sie sich online selbst schützen. Auf der anderen Seite gibt es aber auch Eltern, die sich mit ihrer Technologie zu Hause gut auskennen und den eingesetzten digitalen Sicherheitsmaßnahmen vertrauen – denn 47 Prozent sind der Meinung, dass ihre Kinder zu Hause online sicher sind, weil sie über eine funktionierende Online-Sicherheitssoftware verfügen.

Wie man seine digitale Oase vor unerwünschtem Zugriff schützt

1. **Mit privaten Daten sparen**: Die eigene Online-Privatsphäre ernst nehmen und Informationen weder an Dritte weitergeben noch Zugriff darauf erlauben, damit die Informationen nicht in die falschen Hände geraten.

2. **Software und Betriebssysteme auf dem neuesten Stand halten**, indem die aktuellsten Versionen und Updates direkt installiert werden. Auf diese Weise bleibt ein Gerät vor den neuesten Bedrohungen geschützt.

3. **Stets die Zugriffsrechte der verwendeten Anwendungen überprüfen**, um die Wahrscheinlichkeit zu senken, dass die Daten von Dritten – und darüber hinaus – ohne das eigene Wissen weitergegeben oder gespeichert werden. Es ist immer ratsam, vor der eigentlichen Nutzung einer Anwendung oder eines Dienstes einen zweiten kontrollierenden Blick auf die Zugriffsrechte zu werfen.

4. **Sichere und robuste Passwörter nutzen**. Eine zuverlässige Lösung wie der Kaspersky Password Manager generiert und schützt einzigartige Kennwörter für jedes einzelne Konto. Unbedingt der Versuchung widerstehen, ein und dasselbe Kennwort immer wieder zu verwenden. Jedes Konto erfordert ein einzigartiges Passwort. Zudem sollte das Kennwort mindestens aus 16 Stellen bestehen – inklusive Sonderzeichen und Ziffern. Angebotene Zwei-Faktor-Authentifizierungsmethoden werden insbesondere bei kritischen Diensten stark empfohlen.

5. **Auf allen Windows-, Mac- und Android-Geräten sollte eine IT-Sicherheitslösung installiert sein**. Tools wie Kaspersky Security Cloud integrieren noch weitere nützliche Features wie zum Beispiel den Passwort-Check. Damit können Nutzer herauszufinden, ob ein Passwort, das für den Zugriff auf Online-Konten verwendet wird, gehackt wurde. Die Kontoüberprüfungsfunktion ermöglicht es zudem Konten auf potenzielle Datenlecks zu überprüfen. Wird ein Leck entdeckt, stellt Kaspersky Security Cloud Informationen über die Datenkategorien zur Verfügung, die öffentlich zugänglich sind, so dass die Betroffenen entsprechende Maßnahmen ergreifen können.

Bei Kaspersky erhalten Schüler, Studenten, Dozenten und Lehrer bis zu 50 Prozent Rabatt auf die beliebtesten Lösungen zum Schutz von PCs, Macs oder Android-Mobilgeräten.

Der Kaspersky Student Store befindet sich unter https://www.kaspersky.de/edu

www.kaspersky.de

kaspersky