BERICHT

proofpoint.

BERICHT ZU BENUTZER-RISIKEN

2018

www.proofpoint.com/de

INHALT

Was sind Benutzerrisiken? 4
Methodik des Berichts und Überblick 4
Informationen über die Umfrageteilnehmer 4
Alter und Beruf 4
Verwendete Gerätetypen 4
Grundlegende Cybersicherheitskonzepte 5
Was ist Phishing? 5
Was ist Ransomware? 5
Was ist Malware? 6
Kennwörter und physische Sicherheit 6
Schutz für Ihre gespeicherten und übertragenen Daten 8
Nutzung von Geräten 8
Konsequenzen von Benutzerrisiken 10
Auswirkungen von Cyberkriminalität auf Endbenutzer 10
Auswirkungen von Benutzerrisiken auf Unternehmen 11

WAS SIND BENUTZERRISIKEN?

Riskante Verhaltensweisen von Endbenutzern gefährden weltweit Unternehmen. Die Auswirkungen können sowohl unmittelbar (z. B. eine Ransomware-Infektion) als auch langfristig sein, wenn eine Bedrohung still „auf der Lauer liegt“ (z. B. kompromittierte Anmeldedaten). Wir erleben immer wieder, dass die Gewohnheiten der Benutzer im Umgang mit Cybersicherheit im Privatleben auch das Verhalten am Arbeitsplatz beeinflussen. Gleichzeitig unterschätzen IT-Sicherheitsteams häufig, wie wenig ihre Endbenutzer über grundlegende Cybersicherheitsmaßnahmen wissen.

Diese beiden Faktoren werden durch die Tatsache verschärft, dass die Nutzung von Mobilgeräten und Apps die Trennlinie zwischen privaten und geschäftlichen Verbindungen immer weiter aufweichen lässt. Dies alles zeigt deutlich, dass die Risiken durch Endbenutzer besser definiert und kontrolliert werden müssen. Cyberkriminelle setzen zunehmend auf die Ausnutzung von Endbenutzerfehlern anstelle von Schwachstellen in Hardware, Software und Systemen. Daher müssen Unternehmen einen Cybersicherheitsansatz wählen, der den Menschen im Mittelpunkt hat und auf diese Weise Daten und Ressourcen am effektivsten schützen kann.

METHODIK DES BERICHTS UND ÜBERBLICK

Für unseren zweiten jährlichen *Bericht zu Benutzerrisiken* gaben wir erneut eine Drittanbieter-Umfrage unter arbeitstätigen Erwachsenen in Auftrag. Die Fragen sollten dabei Daten über Endbenutzeraktionen und Kenntnisse im Zusammenhang mit der Sicherheit von Geräten, Daten und Systemen liefern. Wir wiederholten etliche Fragen aus der letztjährigen Umfrage, beleuchteten diesmal jedoch andere Themen genauer, um ein möglichst klares Bild der Kompetenzen arbeitstätiger Erwachsener in folgenden Bereichen zu erhalten:

- Kenntnisse grundlegender Cybersicherheitskonzepte (z. B. Phishing, Ransomware und WLAN-Sicherheit)
- Kennwortmanagement und Bewusstsein für physische Sicherheitsmaßnahmen
- Nutzung von Maßnahmen für Datensicherheit, z. B. VPN (Virtual Private Network) und Datensicherungen
- Anwendung empfohlener Vorgehensweisen bei der Freigabe von Inhalten in sozialen Netzwerken und der Nutzung vom Arbeitgeber überlassener Geräte

Im Gegensatz zur letztjährigen Umfrage (bei der 2.000 arbeitstätige Erwachsene in Großbritannien und den USA befragt wurden), kamen in diesem Jahr mehr als 6.000 arbeitstätige Erwachsene aus sechs Ländern zu Wort: USA, Großbritannien, Deutschland, Frankreich, Italien und Australien. Die hier vorgestellten Ergebnisse spiegeln die weltweiten Durchschnittswerte für alle Teilnehmer wider.

Eine Aufschlüsselung der Umfrageergebnisse nach Ländern finden Sie im Anhang am Ende dieses Berichts.

INFORMATIONEN ÜBER DIE UMFRAGETEILNEHMER

Alter und Beruf

Das Durchschnittsalter der Teilnehmer lag bei etwas über 45 Jahren. An der Umfrage nahmen arbeitstätige Erwachsene aus verschiedensten Tätigkeitsfeldern teil, von ausgebildeten Facharbeitern über Beschäftigte im mittleren öffentlichen Dienst bis hin zu hochrangigen Managern.

Verwendete Gerätetypen

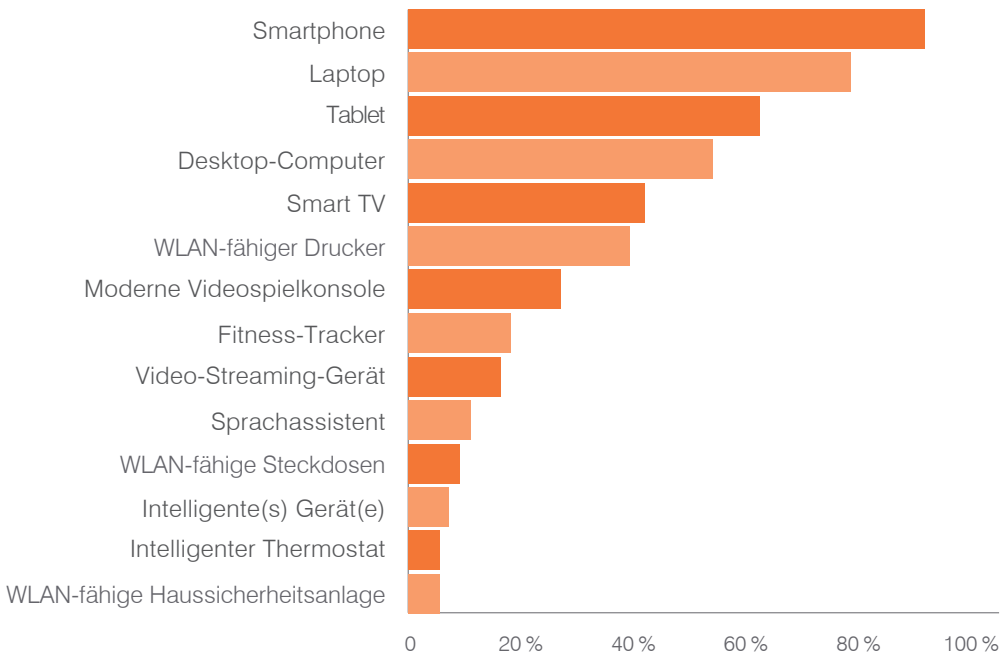
Mehr als 90 % der Umfrageteilnehmer gaben an, dass sie für mobile Kommunikation ein Smartphone nutzen. Im Gegensatz dazu verwenden 7 % ein einfaches Handy, das nur die wichtigsten Funktionen bietet, und weniger als 2 % gaben an, überhaupt kein Mobiltelefon zu besitzen. IT-Sicherheitsteams sollten die Konsequenzen verantwortungslosen Cybersicherheitsverhaltens in Zeiten von BYOD berücksichtigen, da 39 % der befragten Smartphone-Nutzer ihre Geräte sowohl für berufliche als auch für private Zwecke nutzen.

Weniger als 2 % der Umfrageteilnehmer gaben an, in ihrem Haushalt überhaupt keine vernetzten Geräte zu besitzen. Tatsächlich war sogar die Zahl der Umfrageteilnehmer größer, die mehr als 11 Geräte nutzen (3 %).

Wie viele angeschlossene Geräte (Laptops, Smartphones, Tablets, Fitness-Tracker etc.) werden in Ihrem Haushalt genutzt?

0	1–2	3–5	6–10	11+
2 %	27 %	50 %	18 %	3 %

Es ist wenig überraschend, dass Smartphones und Laptops die Gerätekategorie bilden, die am häufigsten mit den Heimnetzwerken der Umfrageteilnehmer verbunden ist. Interessant ist hingegen, dass IoT-Geräte (Internet der Dinge) wie Assistenten, intelligente Geräte und WLAN-fähige Haussicherheitsanlagen weltweit kaum verbreitet sind.



GRUNDLEGENDE CYBERSICHERHEITSKONZEPTE

Es leuchtet ein, dass die sichersten Benutzer ein grundlegendes Verständnis häufiger Cybersicherheitsrisiken besitzen. Leider fehlt zu vielen arbeitstätigen Erwachsenen ausreichendes Wissen über allgemeine Bedrohungen, sodass sie sich zu häufig darauf verlassen, dass andere sich um ihre Sicherheit kümmern.

Was ist Phishing?

67 %	13 %	20 %
Richtig	**Falsch**	**Weiß nicht**

Was ist Ransomware?

36 %	21 %	43 %
Richtig	**Falsch**	**Weiß nicht**

Endbenutzer in Italien und Deutschland wissen am wenigsten über Ransomware. Tatsächlich waren in jedem Land mehr als 50 % der Umfrageteilnehmer nicht bereit, die Antwort auf diese Frage auch nur zu erraten.

Was ist Malware?

68 %	10 %	22 %
Richtig	Falsch	Weiß nicht

Wenn Sie an einem Ort sind, an dem Sie sich sicher fühlen (ein nettes Hotel, ein heimisches Café, ein internationaler Flughafen), dürfen Sie darauf vertrauen, dass ihre Daten im kostenlosen WLAN-Netzwerk sicher geschützt sind.

WAHR	FALSCH
39 %	61 %

Die Antworten der italienischen Endbenutzer waren praktisch gegensätzlich zu den weltweiten Durchschnittswerten: 59 % der Umfrageteilnehmer glaubten, dass offene WLAN-Netzwerke an vertrauenswürdigen Orten sicher wären.

Wenn Sie Antivirensoftware einsetzen und diese auf dem neuesten Stand halten, verhindern Sie damit Cyberangriffe auf Ihren Computer.

WAHR	FALSCH
67 %	17 %

Italienische Endbenutzer setzten viel häufiger ihr (ungerechtfertigtes) Vertrauen in Antivirensoftware: 84 % der Umfrageteilnehmer glauben, dass sie damit Cyberangriffe abwehren können.

Alle geschäftlichen Webseiten werden vor ihrer Veröffentlichung in einem sozialen Netzwerk durch Facebook, Instagram, Twitter etc. überprüft und genehmigt.

WAHR	FALSCH
32 %	68 %

KENNWÖRTER UND PHYSISCHE SICHERHEIT

Kennwörter und physische Sicherheitsmaßnahmen bilden den grundlegendsten Daten- und Geräteschutz – und dennoch haben Benutzer Schwierigkeiten, relativ einfache empfohlene Vorgehensweisen in diesen Bereichen umzusetzen. Die Gefahren durch die Wiederverwendung von Kennwörtern bei Online-Konten wurde in der Öffentlichkeit stark thematisiert. Daher ist es erfreulich, dass ein relativ geringer Anteil der Befragten ohne Kennwortmanager (etwas mehr als 20 %) erklärte, sie würden die gleichen ein bis zwei Kennwörter für alle ihre Konten nutzen. Dennoch stellt auch dieser Anteil eine erhebliche Schwachstelle für Unternehmen dar. Beispielsweise würde er bei einem Unternehmen mit 10.000 Mitarbeitern insgesamt über 2.000 Benutzern entsprechen, die abgesicherte Konten und Systeme erheblich gefährden.

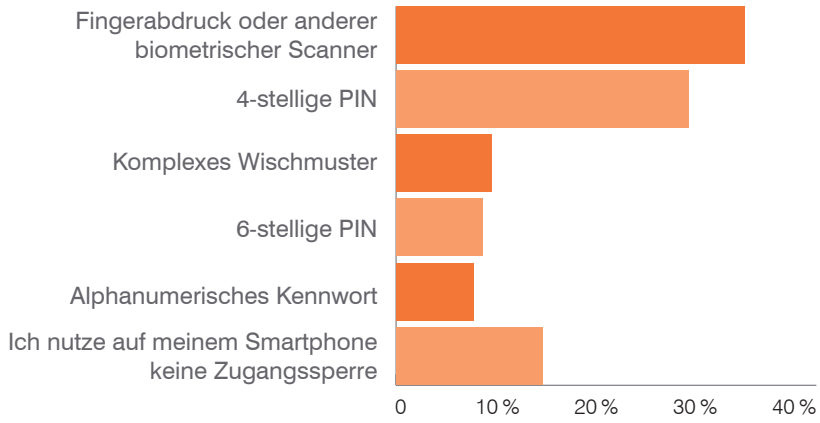
Nutzen Sie einen Kennwortmanager zur Verwaltung Ihrer Online-Kennwörter? (Wählen Sie die am ehesten zutreffende Antwort)

36 %	31 %	26 %	7 %
Nein, ich halte ihn für unnötig	Nein, ich kenne mich mit Kennwortmanagern nicht aus	Ja, denn die Verwaltung all meiner Kennwörter ist damit einfach	Ja, mein Arbeitgeber fordert von mir den Einsatz eines Kennwortmanagers

Falls nein, wie viele Kennwörter nutzen Sie für Ihre Online-Konten? (Wählen Sie die am ehesten zutreffende Antwort)

47 %	32 %	21 %
Ich nutze online zwischen 5 und 10 Kennwörter	Für jedes Konto nutze ich ein anderes Kennwort	Ich verwende die gleichen 1 oder 2 Kennwörter für die meisten/ alle Online-Konten

Welche Art von Zugangssperre setzen Sie auf Ihrem Smartphone hauptsächlich ein?



Mehr als
90 %
der Umfrageteilnehmer verwenden ein Smartphone für mobile Kommunikation.

Wenn Sie sich mit einem Freund oder Kollegen zum Abendessen treffen und Ihr Laptop oder Tablet dabeihaben, dann werden Sie es wahrscheinlich ...

39 %
In Ihren Kofferraum legen

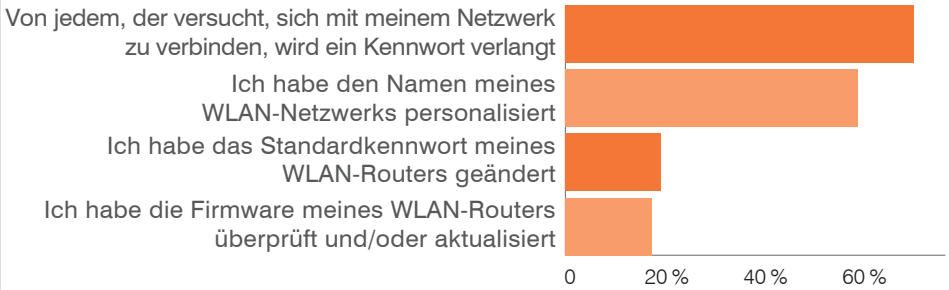
35 %
Mit ins Restaurant nehmen

24 %
Unter einem Mantel oder sonst wie verborgen im Auto zurücklassen

2 %
Offen in Ihrem Auto zurücklassen

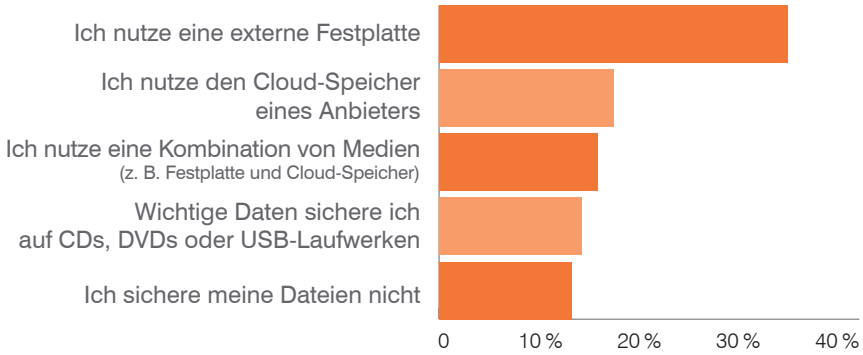
FAKT: Der beste Schutz für Ihr Gerät besteht darin, es stets bei Ihnen zu führen. Der Kofferraum Ihres Autos ist kein sicherer Aufbewahrungsort.

Welche Art von Zugangssperre setzen Sie auf Ihrem Smartphone hauptsächlich ein?



Bei den Umfrageteilnehmern, die diese Sicherheitsmaßnahmen nur teilweise oder überhaupt nicht implementiert hatten, waren 8 % der Meinung, die Prozesse wären zu zeitaufwändig oder nicht praktikabel, und 14 % gaben an, dass ihnen die erforderlichen Informationen fehlen.

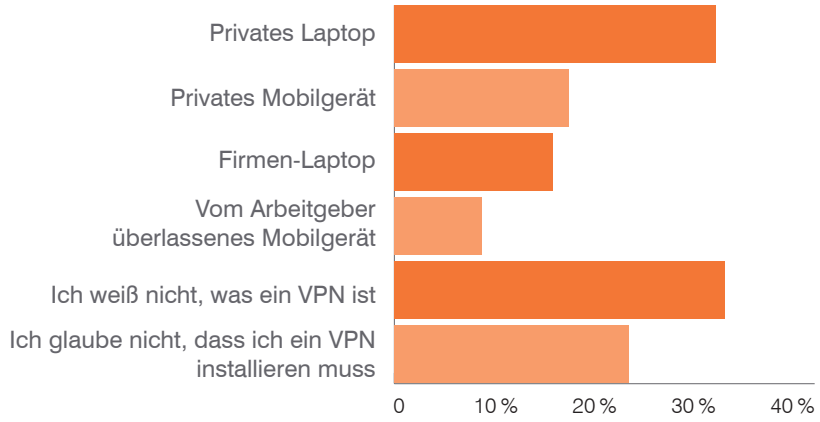
Wie sichern Sie Ihre wichtigen privaten Dateien, digitalen Fotos, Videos usw. Ihres PCs oder Mobilgeräts (Smartphone/Tablet)?



SCHUTZ FÜR IHRE GESPEICHERTEN UND ÜBERTRAGENEN DATEN

Mehr als 90 % der Umfrageteilnehmer sagten, dass sie ein Heim-WLAN-Netzwerk eingerichtet haben. Gleichzeitig ist aus den Antworten erkennbar, dass die Mehrheit dieser Technologienutzer kaum oder keine wichtigen technischen Sicherheitsmaßnahmen implementiert hat. Diese Erkenntnis (zusammen mit den Antworten im Zusammenhang mit VPN-Nutzung) dürfte vor allem Unternehmen mit Mitarbeitern mit Fernzugriff interessieren.

Auf welchen dieser Geräte (sofern zutreffend) ist ein VPN installiert? (Markieren Sie alle zutreffenden)



NUTZUNG VON GERÄTEN

Mit diesen Fragen wollten wir Einblicke darin bekommen, wie frei die Benutzer ihre privaten – und geschäftlichen – Informationen in öffentlichen Kanälen teilen. Auch wollten wir wissen, welche privaten Aktivitäten sie mit Geräten durchführen, die ihnen vom Arbeitgeber überlassen wurden. Soziale Netzwerke sind für die meisten Umfrageteilnehmer eine feste Größe: 51 % gaben an, regelmäßig Beiträge zu veröffentlichen, während sich 30 % als „passive Teilnehmer“ bezeichneten (d. h. sie lesen Beiträge anderer Benutzer, schreiben selbst aber nur selten), und 19 % nutzen nach eigenen Angaben überhaupt keine sozialen Netzwerke. Im Gegensatz dazu nutzen Teilnehmer aus Deutschland erheblich seltener als der weltweite Durchschnitt die sozialen Netzwerke: Nur 35 % posten häufig und 27 % besitzen überhaupt keine Konten bei sozialen Netzwerken.

Überraschend war für uns, dass nur 25 % der weltweiten Umfrageteilnehmer erklärten, sie würden vom Arbeitgeber überlassene Laptops oder Smartphones regelmäßig zu Hause nutzen. Gleichzeitig ist es wahrscheinlich kaum verwunderlich, dass US-amerikanische Mitarbeiter diese Geräte unter allen befragten Umfrageteilnehmern am häufigsten außerhalb des Büros nutzen (35 %).

Wenn Sie ein VPN auf einem Gerät installiert haben, wie oft nutzen Sie es?

39 % Ich setze es immer dann ein, wenn ich mehr Sicherheit benötige

29 % Ich setze es regelmäßig zu Hause und auf Reisen ein

13 % Ich setze es selten/nie ein

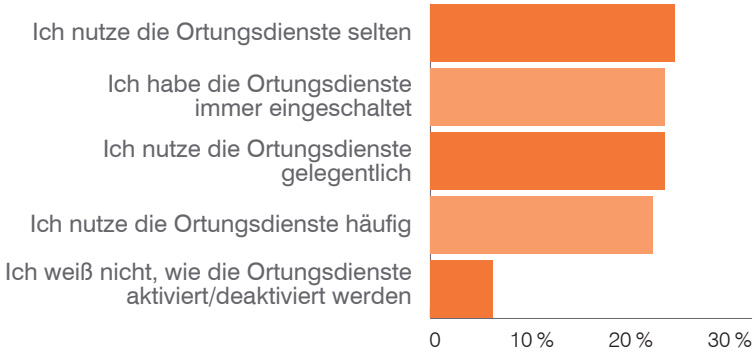
11 % Ich setze es nur ein, wenn ich keine Wahl habe (z. B. für den Zugriff auf geschützte Unternehmenssysteme)

8 % Ich setze es regelmäßig auf Reisen ein

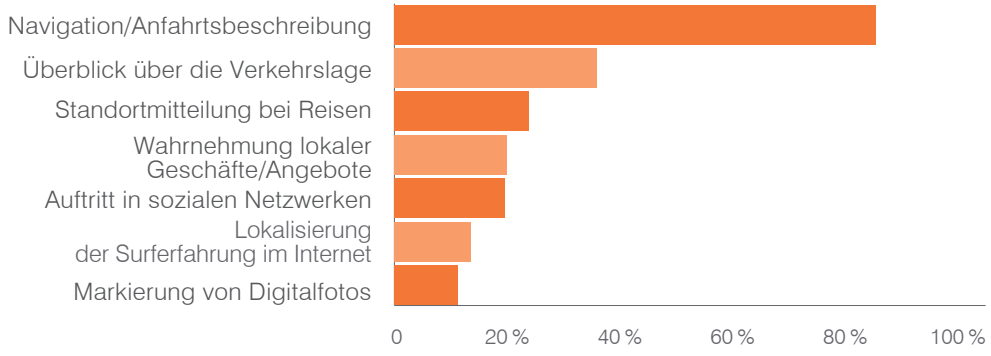
US-amerikanische Technologienutzer hatten nicht nur am häufigsten ein VPN auf mehreren Geräten installiert, sondern sie nutzten diese Technologie auch am stärksten: 49 % gaben an, sie würden bei höheren Sicherheitsanforderungen stets ein VPN einsetzen, und nur 10 % nutzen ihr VPN selten oder nie.

Für IT-Sicherheitsteams liegt die wichtigste Erkenntnis darin, dass arbeitstätige Erwachsene überhaupt kein Problem darin sehen, private Informationen in sozialen Netzwerken zu teilen, und viele Mitarbeiter die Geräte ihrer Arbeitgeber wie ihr Privateigentum behandeln (was zu verschiedenen Problemen führt).

Wie oft aktivieren Sie auf Ihrem Mobilgerät die Ortungsdienste/GPS-Verfolgung? (Wählen Sie die Antwort, die am ehesten zutrifft) Diese Frage ist zweiteilig.



Falls Sie die Standortverfolgung nutzen, in welcher Absicht? (Markieren Sie alle zutreffenden)



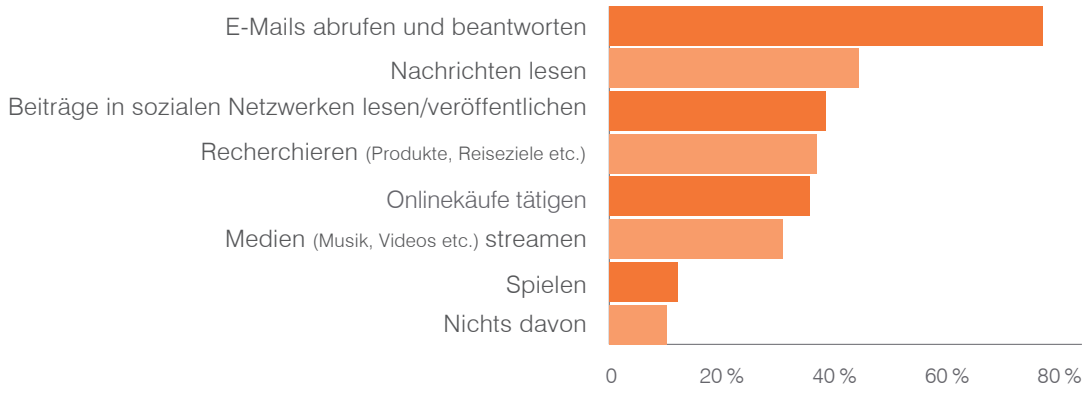
Umfrageteilnehmer aus den USA sind deutlich häufiger als der weltweite Durchschnitt in sozialen Netzwerken aktiv (29 %), und deutsche Teilnehmer teilen am häufigsten ihre Standortdaten auf Reisen (28 %).

Falls Sie regelmäßig Beiträge in sozialen Netzwerken veröffentlichen, welche Art von Inhalt teilen Sie? (Markieren Sie alle zutreffenden)

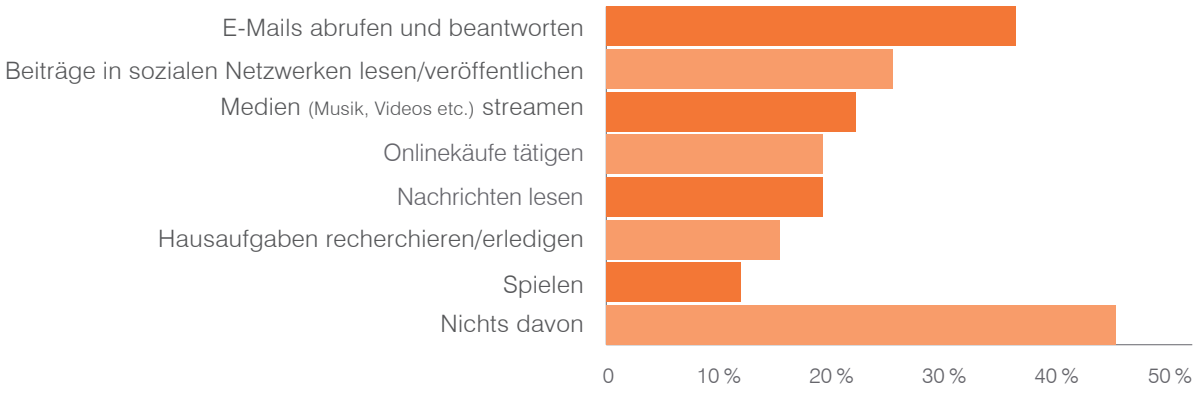
Lustige Meme und Geschichten	Lokale Aktivitäten (z. B. Restaurant-besuche)	Meinen Standort/Auftritt	Private Gedanken und Neuigkeiten	Private Projekte (z. B. Heimwerken, Renovierungen, Handwerk)	Videos und andere Streaming-Medien
33 %	33 %	32 %	32 %	27 %	21 %

Geschäftsreisen	Spezielle Angebote und Deals	Geschäftliche Projekte (z. B. Kundeninitiativen, Produktentwicklung	„Lerne dich kennen“ – Fragen und Antworten	Es gibt fast nichts, was ich nicht in sozialen Netzwerken veröffentlichen würde
18 %	14 %	12 %	6 %	4 %

Welche der folgenden privaten Dinge führen Sie auf Ihrem vom Arbeitgeber überlassenen Gerät aus? (Markieren Sie alle zutreffenden)



Welche Aktivitäten erlauben Sie Familienmitgliedern oder vertrauenswürdigen Freunden auf Ihrem vom Arbeitgeber überlassenen Gerät? (Markieren Sie alle zutreffenden)



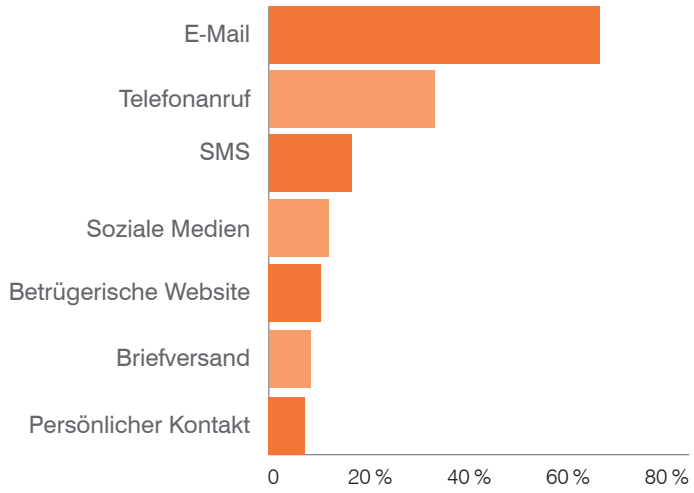
US-amerikanische Teilnehmer nutzen weitaus häufiger als der weltweite Durchschnitt vom Arbeitgeber überlassene Geräte für private Zwecke und gewähren auch Freunden und Familienangehörigen Zugang. Tatsächlich lagen diese Teilnehmer in fast allen Verhaltenskategorien deutlich vor dem weltweiten Durchschnitt und nur 25 % der Angestellten, die vom Arbeitgeber überlassene Geräte zu Hause nutzen, verweigern ihren Freunden und Familienangehörigen den Zugang.

KONSEQUENZEN VON BENUTZERRISIKEN

Auswirkungen von Cyberkriminalität auf Endbenutzer

Endbenutzer wissen offensichtlich, dass Cyberkriminelle auf der Suche nach Opfern sind, auch wenn sie nicht die empfohlenen Verhaltensweisen zum bestmöglichen Schutz ihrer Daten und Geräte nutzen. Mehr als ein Drittel (35 %) der Umfrageteilnehmer gab an, eine Person zu kennen, deren Konto bei einem sozialen Netzwerk gehackt oder dupliziert wurde. 15 % erklärten, sie wären selbst Opfer eines Identitätsdiebstahls geworden (und weitere 9 % sagten, dass sie möglicherweise angegriffen wurden, sich aber nicht sicher wären).

Obwohl 22 % der Teilnehmer sagten, dass sie noch nie eine betrügerische Forderung nach Geld oder persönlichen Daten erhalten hätten (und weitere 8 % sich nicht sicher sind), erklärten die übrigen 70 %, dass sie mit folgenden Mitteln angegriffen wurden: (Die Umfrageteilnehmer sollten alle zutreffenden Antworten markieren.)



Mit **33 %** ist der Anteil der US-Teilnehmer, die bereits Identitätsdiebstahl erlebt haben, mehr als doppelt so hoch wie beim weltweiten Durchschnitt, mehr als dreimal so hoch wie bei deutschen und französischen Teilnehmern und mehr als viermal so hoch wie bei den Befragten in Italien.

Auswirkungen von Benutzerrisiken auf Unternehmen

Obwohl die Umfrage auch einige bemerkenswert positive Erkenntnisse brachte – zum Beispiel, dass fast 70 % der arbeitstätigen Erwachsenen über Phishing und Malware Bescheid wissen –, zeigte sie auch ebenso bemerkenswert negative Erkenntnisse. Dazu gehört, dass nur 37 % der Benutzer das Konzept von Ransomware richtig definieren konnten. Doch selbst die Höhepunkte sind nicht besonders erbaulich. Zum einen zeigen sie den Unternehmen, wie wichtig es ist, bei der Cybersicherheit den Menschen in den Mittelpunkt zu stellen. Zum anderen machen sie deutlich, dass Unternehmen ihre Mitarbeiter zu grundlegenden Verhaltensweisen im Zusammenhang mit Cybersicherheit schulen müssen, um Daten, Geräte und Systeme besser zu schützen.

44 %
der Befragten schützen ihr Heim-WLAN-Netzwerk nicht mit einem Kennwort

66 %
haben das Standardkennwort ihrer WLAN-Router nicht geändert

14 %
der Benutzer haben keine Zugangssperre bei ihren Smartphones

28 %
nutzen eine vierstellige PIN zur Absicherung ihrer Geräte

WENIGER ALS 60 %
der Umfrageteilnehmer gaben zu, dass sie die gleichen Kennwörter für mehrere Online-Konten nutzen

55 %
der arbeitstätigen Erwachsenen, die vom Arbeitgeber überlassene Geräte zu Hause nutzen, erlauben Freunden und Familienmitgliedern den Zugang zu diesen Geräten

Ganz besonders betroffen sind dabei Unternehmen, die BYOD einsetzen bzw. Mitarbeiter mit Fernzugriff haben. Da mehr als 90 % der Umfrageteilnehmer Smartphones nutzen und fast 40 % ihre Geräte für private und berufliche Zwecke verwenden, verschwindet die strikte Grenze zwischen Unternehmens- und Verbrauchersystemen. Die folgenden in unserer Umfrage aufgedeckten Gewohnheiten sind potenzielle Schwachstellen in jedem Unternehmen, dessen Benutzer Zugriff auf geschäftliche Daten und Ressourcen haben, während sie sich außerhalb der IT-Infrastrukturen des Unternehmens befinden:
Wir wissen, dass viele IT-Sicherheitsexperten darüber streiten, welchen Wert Schulungen zur Steigerung des Sicherheitsbewusstseins für Endbenutzer haben: Sind sie den Zeitaufwand überhaupt wert? Lohnt es sich, dafür Budget einzuplanen, das andernfalls für technische Tools genutzt werden könnte? Ist der Erfolg überhaupt sicher?

Sicherlich führen nicht alle Methoden und Programme zu den gewünschten Ergebnissen. Doch wenn Sie den Eindruck haben, dass die Ergebnisse dieses Berichts das Verhalten der Endbenutzer in Ihrem Unternehmen widerspiegeln, sollten Sie stattdessen die folgenden Fragen stellen: Vergrößern schlechte Endbenutzer-Verhaltensweisen das Risiko in Ihrem Unternehmen? Könnten Sie mehr dafür tun, Ihre Benutzer über richtige Cybersicherheit zu schulen? Wenn nicht jetzt – wann dann? Und wenn nicht Sie – wer sonst?

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Wie viele angeschlossene Geräte werden in Ihrem Haushalt genutzt?						
0	3 %	1 %	2 %	1 %	3 %	2 %
1–2	27 %	23 %	26 %	22 %	31 %	37 %
3–5	45 %	47 %	49 %	59 %	51 %	47 %
6–10	21 %	24 %	20 %	16 %	14 %	12 %
11+	4 %	5 %	3 %	2 %	1 %	2 %
Welche Art(en) von angeschlossenen Geräten werden in Ihrem Haushalt genutzt?						
Desktop-Computer	58 %	44 %	53 %	60 %	52 %	52 %
Laptop	79 %	82 %	81 %	61 %	81 %	76 %
Smartphone	86 %	89 %	91 %	96 %	87 %	88 %
Tablet	60 %	71 %	61 %	63 %	58 %	54 %
WLAN-fähiger Drucker	35 %	36 %	32 %	41 %	41 %	41 %
Fitness-Tracker	22 %	24 %	22 %	14 %	10 %	15 %
Intelligente(s) Gerät(e)	11 %	6 %	6 %	9 %	5 %	3 %
Intelligenter Thermostat	11 %	9 %	2 %	6 %	4 %	3 %
Moderne Videospielkonsole	27 %	28 %	22 %	33 %	29 %	20 %
Smart TV	45 %	47 %	40 %	49 %	22 %	44 %
Video-Streaming-Gerät	30 %	19 %	19 %	11 %	6 %	13 %
Sprachassistent	20 %	14 %	10 %	5 %	7 %	10 %
WLAN-fähige Steckdosen	11 %	7 %	9 %	16 %	7 %	8 %
WLAN-fähige Haussicherheitsanlage	11 %	6 %	5 %	8 %	6 %	2 %
Haben Sie ein Heim-WLAN-Netzwerk?						
Ja	91 %	94 %	89 %	91 %	96 %	83 %
Nein	9 %	6 %	11 %	9 %	4 %	17 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Welche der folgenden Aussagen treffen auf Ihr Netzwerk zu? (Markieren Sie alle zutreffenden)						
Ich habe den Namen meines WLAN-Netzwerks personalisiert	58 %	23 %	40 %	42 %	31 %	47 %
Von jedem, der versucht, sich mit meinem Netzwerk zu verbinden, wird ein Kennwort verlangt	58 %	55 %	64 %	55 %	41 %	64 %
Ich habe das Standardkennwort meines WLAN-Routers geändert	37 %	27 %	32 %	43 %	24 %	42 %
Ich habe die Firmware meines WLAN-Routers überprüft und/oder aktualisiert	24 %	16 %	17 %	23 %	11 %	32 %
Ich habe nichts davon getan, weil es zu zeitaufwändig und/oder nicht praktikabel ist	5 %	9 %	7 %	11 %	14 %	5 %
Ich habe nichts davon oder nicht alles getan, weil mir Informationen fehlen	11 %	21 %	14 %	7 %	24 %	5 %
Wenn Sie Antivirensoftware einsetzen und diese auf dem neuesten Stand halten, verhindern Sie damit Cyberangriffe auf Ihren Computer.						
Wahr	61 %	63 %	65 %	84 %	58 %	71 %
Falsch	22 %	20 %	17 %	6 %	22 %	12 %
Weiß nicht	17 %	17 %	18 %	10 %	20 %	17 %
Auf welchen dieser Geräte (sofern zutreffend) ist ein VPN installiert? (Markieren Sie alle zutreffenden)						
Firmen-Laptop	26 %	16 %	15 %	17 %	13 %	17 %
Vom Arbeitgeber überlassenes Mobilgerät	12 %	9 %	7 %	8 %	7 %	9 %
Privates Laptop	32 %	28 %	29 %	31 %	32 %	32 %
Privates Mobilgerät	23 %	21 %	15 %	26 %	15 %	21 %
Ich glaube nicht, dass ich ein VPN installieren muss	19 %	22 %	27 %	18 %	24 %	19 %
Ich weiß nicht, was ein VPN ist	30 %	35 %	32 %	30 %	33 %	33 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Wenn Sie ein VPN auf einem Gerät installiert haben, wie oft nutzen Sie es?						
Ich setze es immer dann ein, wenn ich mehr Sicherheit benötige	49 %	41 %	38 %	38 %	32 %	34 %
Ich setze es regelmäßig zu Hause und auf Reisen ein	25 %	26 %	30 %	29 %	32 %	32 %
Ich setze es regelmäßig auf Reisen ein	8 %	10 %	8 %	7 %	7 %	8 %
Ich setze es nur ein, wenn ich keine Wahl habe (z. B. für den Zugriff auf geschützte Unternehmenssysteme)	8 %	12 %	11 %	14 %	8 %	11 %
Ich setze es selten/nie ein	10 %	11 %	13 %	12 %	21 %	15 %
Wie sichern Sie Ihre wichtigen privaten Dateien, digitalen Fotos, Videos usw. Ihres PCs oder Mobilgeräts (Smartphone/Tablet)?						
Ich nutze eine externe Festplatte	33 %	30 %	38 %	36 %	50 %	45 %
Ich nutze den Cloud-Speicher eines Anbieters	24 %	25 %	16 %	19 %	10 %	13 %
Wichtige Daten sichere ich auf CDs, DVDs oder USB-Laufwerken	10 %	10 %	11 %	16 %	18 %	16 %
Ich nutze eine Kombination von Medien (z. B. Festplatte und Cloud-Speicher)	19 %	19 %	20 %	17 %	10 %	15 %
Ich sichere meine Dateien nicht	14 %	16 %	15 %	12 %	12 %	11 %
Was ist Phishing?						
Richtig	69 %	71 %	62 %	66 %	61 %	72 %
Falsch	14 %	12 %	13 %	11 %	16 %	11 %
Weiß nicht	17 %	17 %	25 %	23 %	23 %	17 %
Nutzen Sie einen Kennwortmanager?						
Ja, denn die Verwaltung all meiner Kennwörter ist damit einfach	39 %	24 %	26 %	27 %	20 %	20 %
Ja, mein Arbeitgeber fordert von mir den Einsatz eines Kennwortmanagers	7 %	7 %	7 %	7 %	7 %	6 %
Nein, ich halte ihn für unnötig	31 %	35 %	32 %	44 %	30 %	45 %
Nein, ich kenne mich mit Kennwortmanagern nicht aus	23 %	34 %	35 %	22 %	43 %	29 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Falls nein, wie viele Kennwörter nutzen Sie für Ihre Online-Konten?						
Für jedes Konto nutze ich ein anderes Kennwort	30 %	33 %	30 %	35 %	28 %	40 %
Ich nutze online zwischen 5 und 10 Kennwörter	48 %	48 %	48 %	46 %	47 %	45 %
Ich verwende die gleichen 1 oder 2 Kennwörter für die meisten/alle Online-Konten	22 %	19 %	23 %	19 %	25 %	15 %
Was ist Ransomware?						
Richtig	41 %	44 %	43 %	29 %	35 %	26 %
Falsch	29 %	23 %	19 %	19 %	20 %	13 %
Weiß nicht	30 %	33 %	38 %	52 %	45 %	61 %
Nutzen Sie ein Smartphone?						
Ja	90 %	91 %	91 %	96 %	90 %	89 %
Nein, ich nutze ein einfaches Handy mit den wichtigsten Funktionen	7 %	7 %	7 %	4 %	9 %	9 %
Nein, ich habe kein Handy	3 %	2 %	2 %	0 %	1 %	2 %
Welche Aussagen beschreiben am ehesten Ihre Nutzung eines Smartphones?						
Ich nutze es ausschließlich aus privaten Gründen	56 %	70 %	52 %	44 %	64 %	71 %
Ich verwende es ausschließlich für Geschäftliches	3 %	1 %	1 %	1 %	2 %	1 %
Ich nutze es sowohl aus privaten als auch aus geschäftlichen Gründen	41 %	29 %	47 %	55 %	34 %	28 %
Welche Art von Zugangssperre setzen Sie auf Ihrem Smartphone hauptsächlich ein?						
Fingerabdruck oder anderer biometrischer Scanner	36 %	36 %	32 %	36 %	28 %	28 %
Komplexes Wischmuster	11 %	9 %	9 %	12 %	9 %	13 %
Alphanumerisches Kennwort	6 %	5 %	5 %	11 %	7 %	6 %
4-stellige PIN	22 %	25 %	25 %	19 %	43 %	34 %
6-stellige PIN	9 %	10 %	11 %	4 %	5 %	8 %
Ich nutze auf meinem Smartphone keine Zugangssperre	16 %	15 %	18 %	18 %	8 %	11 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Wie oft aktivieren Sie auf Ihrem Mobilgerät die Ortungsdienste/GPS-Verfolgung?						
Immer	34 %	24 %	22 %	29 %	21 %	16 %
Häufig	20 %	21 %	19 %	23 %	22 %	17 %
Gelegentlich	20 %	22 %	26 %	27 %	23 %	24 %
Selten	21 %	27 %	25 %	18 %	27 %	34 %
Ich weiß nicht, wie die Ortungsdienste aktiviert/deaktiviert werden	5 %	6 %	8 %	3 %	7 %	9 %
Falls Sie die Standortverfolgung nutzen, in welcher Absicht? (Markieren Sie alle zutreffenden)						
Navigation/Anfahrtsbeschreibung	83 %	80 %	83 %	85 %	82 %	83 %
Überblick über die Verkehrslage	41 %	38 %	31 %	39 %	36 %	39 %
Auftritt in sozialen Netzwerken	29 %	25 %	23 %	19 %	14 %	11 %
Standortmitteilung bei Reisen	24 %	18 %	17 %	25 %	14 %	28 %
Wahrnehmung lokaler Geschäfte/Angebote	26 %	19 %	17 %	23 %	14 %	18 %
Lokalisierung der Surferfahrung im Internet	20 %	16 %	18 %	12 %	9 %	5 %
Markierung von Digitalfotos	10 %	11 %	10 %	11 %	8 %	7 %
Wenn Sie an einem Ort sind, an dem Sie sich sicher fühlen (ein nettes Hotel, ein heimisches Café, ein internationaler Flughafen), dürfen Sie darauf vertrauen, dass ihre Daten im kostenlosen WLAN-Netzwerk sicher geschützt sind.						
Wahr	36 %	32 %	29 %	59 %	45 %	33 %
Falsch	64 %	68 %	71 %	41 %	55 %	67 %
Waren Sie oder jemand, den Sie kennen, bereits das Opfer eines gehackten oder duplizierten Kontos eines sozialen Netzwerks?						
Ja	51 %	35 %	39 %	30 %	32 %	25 %
Nein	49 %	65 %	61 %	70 %	68 %	75 %
Veröffentlichen Sie regelmäßig Beiträge in sozialen Netzwerken?						
Ja, ich poste häufig	32 %	20 %	15 %	24 %	13 %	6 %
Ja, ich poste gelegentlich	34 %	33 %	34 %	36 %	30 %	29 %
Nein, ich sehe mir an, was die anderen schreiben, aber ich selbst trage selten dazu bei	21 %	27 %	33 %	28 %	34 %	38 %
Nein, ich bin bei keinen sozialen Netzwerken	13 %	20 %	18 %	12 %	23 %	27 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Falls ja, welche Art von Inhalt teilen Sie? (Markieren Sie alle zutreffenden)						
Meinen Standort/Auftritt	46 %	41 %	36 %	19 %	22 %	26 %
Geschäftsreisen	24 %	16 %	15 %	22 %	16 %	11 %
Private Reisen	44 %	39 %	50 %	52 %	48 %	39 %
Geschäftliche Projekte	19 %	11 %	11 %	11 %	14 %	8 %
Private Projekte	31 %	29 %	28 %	25 %	23 %	28 %
Lokale Aktivitäten	32 %	35 %	33 %	33 %	29 %	35 %
Bilder von Menschen, Orten und Dingen	50 %	61 %	55 %	57 %	46 %	45 %
Lustige Meme und Geschichten	42 %	39 %	41 %	35 %	17 %	27 %
„Lerne dich kennen“ – Fragen und Antworten	7 %	7 %	6 %	7 %	5 %	5 %
Spezielle Angebote und Deals	16 %	16 %	15 %	15 %	10 %	9 %
Videos und andere Streaming-Medien	26 %	20 %	18 %	25 %	16 %	19 %
Private Gedanken und Neuigkeiten	37 %	31 %	34 %	41 %	18 %	29 %
Es gibt fast nichts, was ich nicht in sozialen Netzwerken veröffentlichen würde	4 %	3 %	3 %	1 %	6 %	6 %
Alle geschäftlichen Webseiten werden vor ihrer Veröffentlichung in einem sozialen Netzwerk durch Facebook, Instagram, Twitter etc. überprüft und genehmigt.						
Wahr	37 %	25 %	26 %	51 %	29 %	24 %
Falsch	63 %	75 %	74 %	49 %	71 %	76 %
Was ist Malware?						
Richtig	66 %	73 %	70 %	80 %	50 %	69 %
Falsch	21 %	9 %	9 %	6 %	7 %	5 %
Weiß nicht	13 %	18 %	21 %	14 %	43 %	26 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Wenn Sie sich mit einem Freund oder Kollegen zum Abendessen treffen und Ihr Laptop oder Tablet dabeihaben, dann werden Sie es wahrscheinlich ...						
Mit ins Restaurant nehmen	35 %	38 %	29 %	42 %	34 %	32 %
Unter einem Mantel oder sonst wie verborgen im Auto zurücklassen	32 %	18 %	37 %	21 %	17 %	19 %
Offen in Ihrem Auto zurücklassen	2 %	1 %	2 %	1 %	3 %	3 %
In Ihren Kofferraum legen	31 %	43 %	32 %	36 %	46 %	46 %
Haben Sie ein vom Arbeitgeber überlassenes Laptop, das Sie regelmäßig zu Hause nutzen?						
Ja	35 %	23 %	22 %	31 %	19 %	17 %
Nein	65 %	77 %	78 %	69 %	81 %	83 %
Welche der folgenden PRIVATEN Dinge führen Sie auf Ihrem vom Arbeitgeber überlassenen Gerät aus? (Markieren Sie alle zutreffenden)						
E-Mails abrufen und beantworten	81 %	64 %	78 %	87 %	77 %	66 %
Beiträge in sozialen Netzwerken lesen/ veröffentlichen	48 %	38 %	39 %	39 %	39 %	28 %
Medien (Musik, Videos etc.) streamen	40 %	28 %	28 %	23 %	21 %	23 %
Onlinekäufe tätigen	42 %	35 %	29 %	37 %	28 %	27 %
Nachrichten lesen	38 %	38 %	38 %	60 %	36 %	47 %
Recherchieren (Produkte, Reiseziele etc.)	29 %	30 %	34 %	42 %	35 %	36 %
Spielen	24 %	14 %	11 %	15 %	13 %	9 %
Nichts davon	5 %	17 %	11 %	5 %	5 %	16 %

ANHANG: AUFSCHLÜSSELUNG DER UMFRAGEERGEBNISSE NACH LÄNDERN

	USA	Großbritannien	Australien	Italien	Frankreich	Deutschland
Haben Sie schon einmal eine betrügerische Forderung nach Geld oder privaten Daten über die folgenden Medien erhalten? (Markieren Sie alle zutreffenden)						
E-Mail	72 %	62 %	65 %	54 %	70 %	49 %
Telefonanruf	47 %	27 %	39 %	14 %	25 %	15 %
Persönlicher Kontakt	11 %	5 %	6 %	7 %	5 %	4 %
Soziale Medien	19 %	10 %	11 %	9 %	11 %	6 %
SMS	24 %	16 %	31 %	14 %	12 %	6 %
Betrügerische Website	12 %	6 %	8 %	11 %	12 %	12 %
Briefversand	15 %	8 %	8 %	3 %	5 %	7 %
Ich habe noch nie eine betrügerische Aufforderung erhalten	14 %	22 %	19 %	32 %	16 %	26 %
Mir ist nicht bekannt, dass ich schon mal eine betrügerische Aufforderung erhalten hätte	5 %	9 %	7 %	6 %	6 %	14 %
Wurden Sie jemals Opfer eines Identitätsdiebstahls (d. h. jemand hat Ihre personenbezogenen Daten gestohlen und diese genutzt, um sich unter Ihrem Namen finanziell zu bereichern)?						
Ja	33 %	17 %	13 %	8 %	10 %	9 %
Nein	60 %	77 %	77 %	81 %	83 %	80 %
Weiß nicht	7 %	6 %	10 %	11 %	7 %	11 %

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.