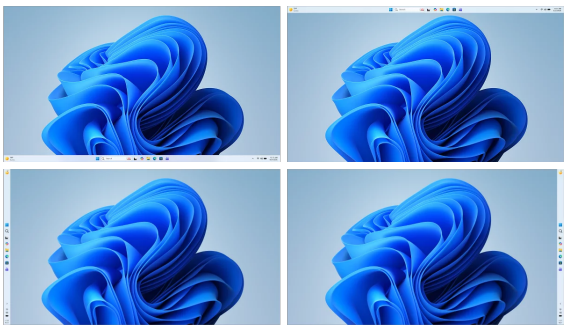
In vielen Foren klagen User über nachlassende Qualität der Apple-Software, und man munkelt, dass sich eine bevorstehende macOS-Version wie ein neues „Snow Leopard" in erster Linie der Qualitätsverbesserung widmen werde. Nun, schauen wir einmal über den Apple-Tellerrand hinaus in die Windows-Welt. Da überraschte Windows-Chef Pavan Davuluri letzte Woche mit einer Mail an Windows-Insider, die, wenn man über die enthaltenen Schönfärbereien hinwegliest, eine Menge an Mängeln eingesteht. Hier ist der Wortlaut:

Unser Anspruch an die Windows-Qualität

Hallo Windows-Insider,

ich möchte mich direkt an Sie wenden. Ich habe meine Karriere damit verbracht, Technologien zu entwickeln, auf die Menschen täglich angewiesen sind. Windows berührt mehr Menschen als fast jede andere Technologie auf der Welt. Jeden Tag hören wir von der Community, wie Sie Windows erleben. In den letzten Monaten haben mein Team und ich viel Zeit damit verbracht, Ihr gesamtes Feedback zu analysieren. Dabei wurde deutlich: Ihnen liegt Windows sehr am Herzen und Sie wollen, dass es noch besser wird.

Heute möchte ich Ihnen zeigen, wie wir auf das Feedback reagieren. Einige der ersten Änderungen werden wir noch in diesem Monat und im Laufe des Aprils in Builds für Windows-Insider vorstellen.



Mehr Anpassungsmöglichkeiten für die Taskleiste, einschließlich vertikaler Positionen und einer Position am oberen Bildschirmrand Die Möglichkeit, die Taskleiste zu verschieben, war einer der am häufigsten geäußerten Wünsche. Wir führen nun die Funktion ein, sie an den oberen oder seitlichen Bildschirmrand zu verschieben, damit Sie Ihren Arbeitsbereich leichter anpassen können.

KI gezielt dort integrieren, wo es am sinnvollsten ist – mit Sorgfalt und Fokus Sie werden merken, dass wir genau überlegen, wie und wo Copilot in Windows zum Einsatz kommt. Der Fokus liegt auf Funktionen, die wirklich nützlich sind und sorgfältig gestaltet wurden. Gleichzeitig reduzieren wir unnötige Einstiegspunkte für Copilot, beginnend bei Apps wie Snipping Tool, Fotos, Widgets und Editor.

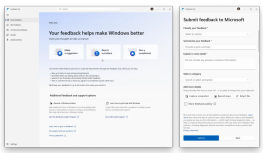
Weniger Unterbrechungen durch Windows Updates
Updates sollten vorhersehbar sein und sich gut einplanen lassen. Deshalb geben wir Ihnen mehr Kontrolle. Sie können Updates beim Einrichten des Geräts überspringen, um schneller auf den Desktop zu gelangen, Ihre Geräte neu starten oder herunterfahren, ohne Updates durchzuführen, und Updates bei Bedarf länger pausieren. Gleichzeitig reduzieren wir unnötige Unterbrechungen durch weniger automatische Neustarts und Benachrichtigungen.

Schnellerer und zuverlässigerer Datei-Explorer
Der Datei-Explorer gehört zu den am häufigsten genutzten Bereichen in Windows. Unsere ersten Verbesserungen konzentrieren sich auf ein schnelleres Startverhalten, weniger Flackern, eine flüssigere Navigation und eine zuverlässigere Leistung bei alltäglichen Dateioperationen.

Mehr Kontrolle über Widgets und Feed-Erlebnisse
Widgets sollen hilfreich und relevant sein, statt Sie abzulenken oder zu überwältigen. Wir führen zurückhaltendere Voreinstellungen ein, geben Ihnen mehr Kontrolle darüber, wann und wie Widgets angezeigt werden, und verbessern die Personalisierung im Discover-Feed.

Ein einfacheres und transparenteres Windows-Insider-Programm Das Windows Insider-Programm ist Ihre Möglichkeit, die Zukunft von Windows mitzugestalten. Dabei sollte klar verständlich sein, was Sie erwarten können und wie Sie teilnehmen. Wir führen Änderungen ein, die Ihnen die Orientierung erleichtern: eine klare Kanalstruktur, einen einfacheren Zugriff auf neue Funktionen, hochwertigere Builds, mehr Transparenz darüber, wie Ihr Feedback Windows beeinflusst, und mehr Möglichkeiten, direkt mit uns zu interagieren.

Besserer Feedback-Hub — ab sofort verfügbar Ihr Feedback ist entscheidend für die Weiterentwicklung von Windows. Es sollte einfach sein, Feedback zu geben und zu sehen, was andere sagen. Heute führen wir für Windows-Insider das bisher größte Update des Feedback-Hubs ein: eine neu gestaltete Oberfläche, die das Einreichen von Feedback und den Austausch mit der Community schneller und einfacher macht.



Aufbauend auf diesen Änderungen stellen wir Ihnen unseren Plan und unsere Schwerpunkte für dieses Jahr vor, um die Qualität von Windows 11 weiter zu steigern. Die Arbeit daran ist bereits in vollem Gange und Sie werden beim Testen unserer Builds im Laufe des Jahres spürbare Fortschritte erleben.

[Vor kurzem] hatte ich die Gelegenheit, hier in Seattle eine kleine Gruppe von Windows-Insidern zu treffen, ihnen zuzuhören, Fragen zu beantworten und mehr über unsere zukünftige Ausrichtung zu berichten. Das Treffen in Seattle war die erste von mehreren Stationen, die unser Team weltweit besuchen wird, um die Windows-Community persönlich kennenzulernen und sich auszutauschen.

Vielen Dank, dass Sie hohe Ansprüche an uns stellen! Windows gehört genauso Ihnen wie uns. Wir möchten seine Basis stärken und Innovationen dort einführen, wo sie wirklich zählen.

Bitte senden Sie uns weiterhin Ihr Feedback, damit wir gemeinsam die Zukunft von Windows gestalten können.

Pavan Davuluri
EVP, Windows & Devices

Leistung, Zuverlässigkeit, Ausführung auf höherem Niveau

Wir möchten Ihnen unseren Plan vorstellen, die Qualität von Windows 11 in diesem Jahr weiter zu steigern. Dabei liegt der Fokus auf **Leistung, Zuverlässigkeit und sorgfältig gestalteten Erlebnissen**. Diese Bereiche bestimmen direkt, wie Sie Windows erleben, wie schnell es startet und reagiert, wie stabil es im Alltag unter realen Bedingungen läuft und wie konsistent und durchdacht die Nutzung insgesamt wirkt.

LEISTUNG

Wir konzentrieren uns darauf, Windows 11 reaktionsschneller und konsistenter zu machen, damit sich die Leistung flüssig und zuverlässig anfühlt.

Im Laufe des Jahres verbessern wir die Systemleistung, die Reaktionsgeschwindigkeit von Apps, den Datei-Explorer und das Windows-Subsystem für Linux. So bleibt Windows auch beim Wechsel zwischen verschiedenen Apps und Aufgaben schnell und stabil.

Systemleistung verbessern:
Weniger Ressourcenverbrauch von Windows bedeutet mehr Leistung für Ihre Aufgaben

Schnellere und reaktionsschnellere Windows-Erlebnisse, mit ersten Verbesserungen, die bereits zu kürzeren Startzeiten bei Apps wie dem Datei-Explorer führen

Bessere Speichereffizienz, Senkung des Grundverbrauchs an Arbeitsspeicher von Windows und die Freigabe von mehr Kapazität für die von Ihnen genutzten Apps

Konstantere Leistung auch unter Last, sodass Apps den ganzen Tag über reaktionsschnell bleiben

Flüssigere und reaktionsschnellere App-Interaktionen:
Verringerung der Reaktionszeiten durch die Migration zentraler Windows-Erlebnisse auf das WinUI3-Framework

Verbesserung der gemeinsamen UI-Infrastruktur, auf die Windows-Erlebnisse angewiesen sind, zur Reduzierung von Reaktionszeiten und des Plattform-Overheads

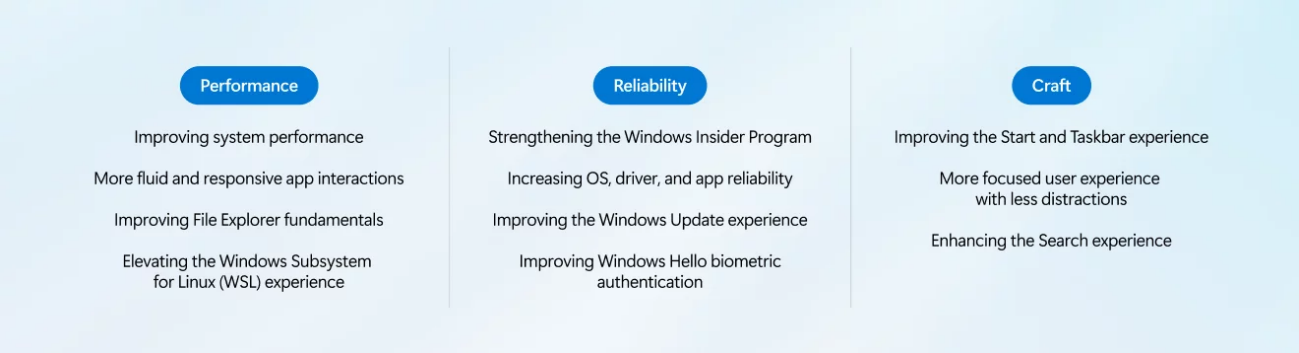
Schnellere Reaktionszeiten in zentralen Windows-Erlebnissen wie dem Startmenü durch die Umstellung weiterer Elemente auf WinUI3

Verbesserung der Grundlagen des Datei-Explorers:
Reduzierung von Verzögerungen und Steigerung der Zuverlässigkeit bei der Suche, Navigation und den Dateioperationen

Deutlich geringere Verzögerungen bei der Suche, Navigation und in Kontextmenüs

Schnelleres und zuverlässigeres Kopieren und Verschieben großer Dateien

Schnellere Startzeiten und Reaktionszeiten bei gängigen Dateioperationen



Verbesserung des Windows-Subsystems für Linux (WSL): Steigerung der Leistung, Zuverlässigkeit und Integration für Entwickler, die Linux-Tools und -Umgebungen unter Windows nutzen

Schnellere Dateioperationen zwischen Linux und Windows

Verbesserte Netzwerkkompatibilität und Datendurchsatz

Einfachere Erstkonfiguration und Onboarding-Erlebnis

Bessere Unternehmensverwaltung durch stärkere Richtlinienkontrolle, Sicherheit und Governance

ZUVERLÄSSIGKEIT

Zuverlässigkeit ist die Grundlage von Vertrauen. Sie sollten darauf vertrauen können, dass Ihr PC zuverlässig funktioniert, wenn Sie ihn am dringendsten benötigen.

Wir werden uns im gesamten Betriebssystem darauf konzentrieren, die grundlegende Zuverlässigkeit in Bereichen wie dem Windows-Insider-Programm, Treibern und Apps, Updates sowie Windows Hello zu verbessern.

Stärkung der Zuverlässigkeit und Qualität des Windows-Insider-Programms: Klarere Erwartungen für jeden Insider-Kanal, höhere Qualitätsstandards für die Builds und verbesserte Feedback-Signale, um die Build-Qualität vor der Veröffentlichung zu erhöhen

Bessere Übersicht darüber, welche Funktionen in jedem Insider-Build enthalten sind, damit Sie wissen, was Sie erwartet

Mehr Kontrolle darüber, welche neuen Funktionen Sie ausprobieren, mit einfacherem Wechsel zwischen den Insider-Kanälen, um den gewünschten Stabilitätsgrad oder frühen Zugriff zu erhalten

Höherwertige Builds in jedem Kanal, mit rigoroserer Validierung und Feedback-Signalen vor der Veröffentlichung

Stärkere Feedback-Schleifen in Windows, damit Probleme schneller erkannt, priorisiert und behoben werden

Steigerung der Zuverlässigkeit des Betriebssystems, der Treiber und der Apps: Wir sorgen für ein flüssigeres und verlässlicheres Windows-11-Erlebnis, indem wir die Systemstabilität, Treiberqualität und App-Zuverlässigkeit im gesamten Ökosystem aus Silicon-, ISV- und OEM-Partnern *[verbessern]*. Unsere Prioritäten sind:

Stärkung der Windows-Basis durch die Reduzierung von Betriebssystemabstürzen sowie die Verbesserung der Treiberqualität und App-Stabilität im gesamten Ökosystem, damit PCs jeden Tag reibungslos und zuverlässig laufen

Einfachere, schnellere und stabilere Verbindungen mit Bluetooth-Zubehör, weniger USB-Abstürze und Verbindungsverluste sowie verbesserte Druckererkennung und -Verbindungen

Zuverlässigere Kamera- und Audioverbindungen für mehr Produktivität bei der Arbeit und in der Freizeit

Konsistenteres Aufwachen der Geräte, einschließlich zusätzlicher Verbesserungen für Docking-Szenarien, damit Sie schneller wieder mit der Arbeit starten können

Verbesserung der Windows-Updates: Schnellere, besser planbare Updates mit klarerer Steuerung von Neustarts und Update-Zeitpunkten

Weniger Unterbrechungen durch Windows Update: Geräte werden auf einen monatlichen Neustart umgestellt, während Organisationen und Nutzer, die neue Funktionen und Fixes schneller erhalten möchten, weiterhin die Möglichkeit dazu haben

Mehr direkte Kontrolle über Updates, einschließlich der Möglichkeit, Updates beliebig lange zu pausieren und Geräte neu zu starten oder herunterzufahren, ohne Updates durchzuführen

Schnellere und verlässlichere Updates mit klarerem Fortschritt während der Updates und integrierter Wiederherstellung, falls etwas schiefgeht

Verbesserung der biometrischen Windows Hello-Anmeldung: Wir stärken Windows Hello, damit die Anmeldung zuverlässig, mühelos und sicher funktioniert. Reibungsverluste werden reduziert und Sie können darauf vertrauen, dass Ihr Gerät Sie korrekt erkennt.

Zuverlässigere Gesichtserkennung, damit die Anmeldung reibungslos funktioniert

Schnellere und verlässlichere Anmeldung per Fingerabdruck mit weniger Wiederholungen

Einfachere sichere Anmeldung auf Gaming-Handhelds wie dem ROG Xbox Ally X, mit vollständiger Gamepad-Unterstützung zur Festlegung einer PIN während der Einrichtung und in den Einstellungen

AUSFÜHRUNG

Für uns ist die Ausführung die Disziplin, die funktionale Produkte durch Benutzerfreundlichkeit, Feinschliff, Kohärenz und Ausgereiftheit zu Produkten macht, die Nutzer lieben.

In diesem Jahr werden Sie sehen, dass wir in die Verbesserung der allgemeinen Benutzerfreundlichkeit investieren. Dazu gehören mehr Möglichkeiten zur Personalisierung, weniger Ablenkung, weniger störende Elemente und mehr Kontrolle über das gesamte Betriebssystem. Außerdem gehen wir sorgfältig damit um, wie und wo wir KI in Windows integrieren. Transparenz, Wahlfreiheit und Kontrolle stehen dabei im Vordergrund, damit neue Funktionen das Erlebnis bereichern, statt zu erschweren.

Verbesserung des Startmenüs und der Taskleiste: Diese zentralen Windows-Oberflächen werden zuverlässiger, flexibler und persönlicher, damit Sie Ihren PC so nutzen können, wie es für Sie am besten passt.

Das Startmenü und die Taskleiste bieten noch konsistenteren und zuverlässigeren Zugriff auf Apps und Dateien, sodass der Wechsel zwischen Ihren Inhalten den ganzen Tag über flüssig bleibt

Erweiterte Personalisierungsoptionen für die Taskleiste, einschließlich alternativer Positionen und einer kleineren Taskleiste, damit Sie diese zentrale Fläche besser an Ihren Arbeitsablauf anpassen können

Der Bereich „Empfohlen“ im Startmenü zeigt künftig die Apps und Inhalte, die Ihnen am wichtigsten sind, und lässt sich mit klaren Einstellungen anpassen oder ganz deaktivieren

Mehr Fokus durch weniger Ablenkung: Windows wird insgesamt ruhiger, damit Sie konzentriert bleiben, Ablenkungen minimieren und im Arbeitsfluss bleiben können.

Die Einrichtung neuer Windows-PCs ist ruhiger und schlanker, mit weniger Schritten und Neustarts, sodass der Einstieg einfacher fällt

Widgets zeigen Informationen standardmäßig gezielter an, bleiben gut überschaubar und vermeiden unnötige Unterbrechungen

Einfachere Einstellungen erleichtern die Personalisierung sowie das Aktivieren oder Deaktivieren von Widgets und Feed-Inhalten nach Ihren Vorlieben

Weniger Benachrichtigungen helfen Ihnen, den ganzen Tag konzentriert zu bleiben

Verbesserung der Suche: Schnellere und präzisere Ergebnisse bei einem konsistenten Sucherlebnis über alle Windows-Oberflächen hinweg.

Finden Sie schneller, was wichtig ist. Die Suche zeigt Apps, Dateien und Einstellungen klar an, sodass Sie direkt zum richtigen Ergebnis gelangen

Ergebnisse sind klarer und vertrauenswürdiger. Inhalte auf Ihrem Gerät sind leicht verständlich und deutlich von Web-Ergebnissen getrennt

Konsistentes Sucherlebnis in der Taskleiste, im Startmenü, im Datei-Explorer und in den Einstellungen

Basierend auf Ihrem Feedback entwickeln wir Windows hinter den Kulissen weiter, um die Qualität spürbar zu steigern und Innovation dort zu schaffen, wo sie für Sie den größten Unterschied macht.

Dazu gehören gründlichere Prüfungen und umfangreiche Tests auf echter Hardware und in realen Nutzungsszenarien, bevor neue Funktionen zu den Windows-Insidern gelangen, sowie ein gezielter Ansatz, wo und wie neue Möglichkeiten eingeführt werden. Das Ergebnis sind qualitativ hochwertigere Builds, sinnvollere Innovationen und mehr Flexibilität bei der Auswahl der Funktionen, die Sie ausprobieren möchten. So entwickeln wir Windows 11 weiterhin jeden Monat weiter und sorgen dafür, dass Sie mit noch mehr Zuversicht bessere Erfahrungen machen.

Im Rahmen der Secure-Future-Initiative von Microsoft machen wir Windows mit jeder Version sicherer. Wir integrieren neue Funktionen und stärken die Sicherheit standardmäßig, um Nutzer, Geräte und Daten bestmöglich zu schützen.

Wir freuen uns darauf, auch weiterhin von Ihnen zu hören, damit wir Windows Schritt für Schritt noch besser machen können.

Mein Dank gilt allen Lesern, die mir helfen, die MACtreff-Köln-Homepage und den Newsletter zu finanzieren.

Wer meine Arbeit unterstützen möchte, kann das durch eine Spende auf mein Paypal-Konto tun:
paypal.me/KJM54

Betrüger wollen unsere Daten, aber viele von uns schützen unsere Geräte nicht

Quelle: Dashia Milden, CNET • Grafiken: Tharon Green, CNET • Übersetzung: Apple und KJM

Antivirensoftware ist nur ein Teil des Schutzes unserer Telefone und Laptops. Sie benötigen eine Kombination von Tools, um Ihre Online-Sicherheit und Ihren Datenschutz zu verbessern.

Betrüger werden niemals eine Gelegenheit verpassen, Malware zu verwenden, um Ihre Daten zu stehlen. Während wir das Internet für fast alles nutzen, vom Bankwesen bis hin zu sozialen Medien, erzeugen sie täglich Tausende neuer Viren, um die Aktivitäten anzusprechen, die Sie am meisten ausüben.

Vielleicht haben wir uns online zu wohl gefühlt und nach den üblichen roten Fahnen wie verdächtigen Links und Rechtschreibfehlern gesehen. Und wir haben Antivirensoftware vertraut, um uns vor diesen hinterhältigen Versuchen zu schützen, bösartige Software zu installieren, die unsere persönlichen Daten in Sekundenschnelle sammeln kann. Die neuesten Ergebnisse von CNET zeigen, dass Betrüger trotz Fortschritten bei Antivirensoftware und anderen Cybersicherheitstools immer noch Wege finden, die Antivirensoftware zu umgehen, der wir vertrauen.

Mehr als die Hälfte (54 %) der Erwachsenen in den USA mit persönlichen Laptops ist im vergangenen Jahr auf potenzielle Malware auf diesen Geräten gestoßen. Es mag Sie überraschen zu erfahren, welche Malware-Bedrohung die Hauptrolle spielt und was Laptop-Besitzer tun, wenn sie auf potenzielle Malware stoßen.

Was Sie tun, wenn Sie auf einen bösartigen Link, eine E-Mail oder einen App-Download stoßen, ist das Wichtigste. Das Ignorieren eines Pop-ups oder das Klicken auf einen Link aus Neugierde kann zu einem Virus, Identitätsdiebstahl und sogar Betrug führen.

Wir können Ihnen helfen, diese Instanzen zu umgehen. Hier sind die neuesten Umfrageergebnisse von CNET und inwieweit die Experten von CNET sagen, dass Antivirensoftware Sie wirklich vor Phishing-Kopfschmerzen und Ärger schützen kann.

Wichtige Ergebnisse

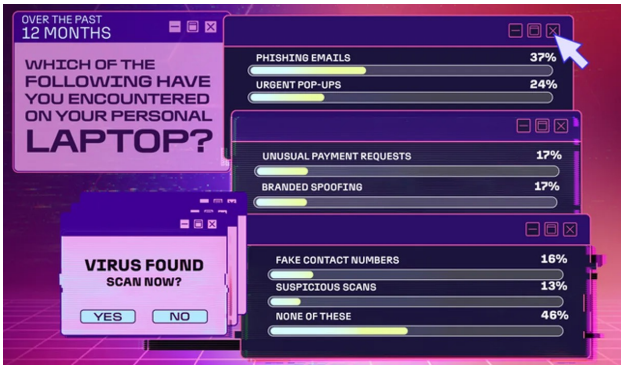
- 78 % der Erwachsenen in den USA besitzen derzeit einen persönlichen Laptop. Mehr als die Hälfte der Laptop-Marken, die Erwachsene in den USA besitzen, sind HP (32 %) und Apple (26 %).
- Mehr als die Hälfte (54 %) der Laptop-Besitzer ist in den letzten 12 Monaten auf potenzielle Malware auf ihrem persönlichen Laptop gestoßen.
- 88 %, die in den letzten 12 Monaten angaben, potenzielle Malware gesehen zu haben, haben etwas dagegen getan, während 12 % nichts dagegen unternommen haben.
- 68 % der Laptop-Besitzer, die Maßnahmen ergriffen haben, haben entweder die Datei gelöscht oder die verdächtige Website oder das Pop-up geschlossen.
- 37 % der Laptop-Besitzer haben in den letzten 12 Monaten Phishing-E-Mails erhalten.

Laptop-Besitzer sind am meisten auf Phishing-E-Mails gestoßen

Meine Mutter hat gerade einen neuen Laptop bekommen und mir gesagt, dass sie keinen Virenschutz braucht. Sie hat nicht ganz Unrecht. Die Antiviren-Experten von CNET, Moe Long und Attila Tomaschek, sagen, dass Sie nicht unbedingt ein weiteres Antivirenprogramm benötigen, wenn Ihr Gerät bereits über einen integrierten Antivirenschutz verfügt — wie es die meisten Computer heute tun.

Windows 11 enthält Microsoft Defender Antivirus-Schutz. Mac-Benutzer haben XProtect, um nach Malware zu suchen, während das Malware-Entfernungstool alles abfängt, was XProtect möglicherweise übersehen hat. Und die Gatekeeper-Funktion verhindert, dass Sie Apps und Software öffnen, denen Sie nicht vertrauen. Aber Viren, Phishing- und Malware-Versuche lauern immer noch, wie die Studie von CNET zeigt.

CNET stellte fest, dass im vergangenen Jahr Erwachsene in den USA, die einen Laptop besitzen, am häufigsten auf Phishing-E-Mails gestoßen sind oder mit ihnen interagiert haben (37 %), gefolgt von dringenden Pop-ups (24 %), ungewöhnlichen Zahlungsanfragen (17 %) und Marken-Spoofing (17 %).



Cyberkriminelle nutzen künstliche Intelligenz, um Betrug glaubwürdiger zu machen — sogar durch Identitätsbetrug. Und sie entwickeln neue Taktiken viel schneller als in den 1990er Jahren, als wir alle unsere Desktops nach dem erfolgreichen Malware-Angriff eines Betrügers zu Geek Squad brachten, um Hilfe zu erhalten.

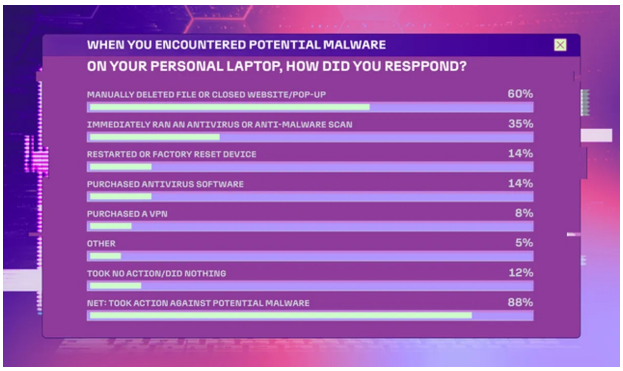
Aber hier ist der wichtigste Unterschied, den es zu wissen gilt: Antivirensoftware kann möglicherweise nicht helfen, Phishing- und Malware-Versuche zu identifizieren, die sich ständig weiterentwickeln. Es kann verhindern, dass bösartige Software Ihr Gerät und Ihre persönlichen Daten angreift, solange sich diese Malware in der Datenbank bekannter Bedrohungen befindet. Aber Sie müssen zuerst Ihr bestes Urteilsvermögen verwenden, um zu vermeiden, dass Sie auf diese verdächtigen Links klicken.

88 % der US-Erwachsenen ergriffen Maßnahmen, nachdem sie potenzielle Malware gesehen hatten

CNET stellte fest, dass 88 % der US-Erwachsenen, die Laptops besitzen, Maßnahmen ergriffen haben, nachdem sie im vergangenen Jahr auf potenzielle Malware gestoßen sind. Das sind ermutigende Neuigkeiten für Long und Tomaschek.

„Sie wollen nicht wirklich mit Malware herumspielen, vor allem nicht mit der Art und Weise, wie viele moderne Malware entwickelt wurden, um Ihre Daten zu erhalten, anstatt Ihren Computer abzustürzen zu lassen oder so etwas“, sagt Long.

Hier ist ein genauerer Blick darauf, wie Laptop-Besitzer Maßnahmen ergreifen.



Über die Hälfte (60 %) der Erwachsenen in den USA hat die Datei entweder manuell gelöscht oder eine Website oder ein Pop-up geschlossen, und 35 % haben sofort einen Antiviren- oder Anti-Malware-Scan durchgeführt. Long sagt jedoch, dass einige dieser Aktionen effektiv und hilfreich sind, während andere es nicht sind.

Wenn es ein bösartiges Pop-up gibt und Sie es schließen, ohne auf einen Link zu klicken, müssen Sie sich möglicherweise keine Sorgen um Malware oder einen Virus machen, sagt Long. Wenn Sie eine bösartige Datei herunterladen, können Sie sie möglicherweise löschen, bevor sie Schaden anrichtet. Aber wenn Sie eine ausführbare Datei herunterladen, wie z. B. eine Softwareanwendung, die Ihr Gerät infiziert, wenn sie ausgeführt wird, könnten Sie tatsächlich Malware auf Ihrem Computer installieren, zusammen mit dem, was Sie für nur eine Anwendung halten.

Einige Maßnahmen sind auf jeden Fall ergreifenswert, wie die sofortige Durchführung eines Antiviren- oder Anti-Malware-Scans nach dem Auffinden von Malware (35 %), sagt Long.

Aber andere Aktionen sind es nicht, wie die Installation eines VPN, was laut CNET 8 % der US-Laptopbesitzer tun.

Long sagt, dass ein VPN ein Datenschutz-Tool ist und nur sehr wenige Sicherheitsvorteile hat. Wenn Sie ein VPN in einem öffentlichen WLAN-Netzwerk verwenden, das angegriffen wird, kann ein VPN das Risiko mindern, dass der Angriff Ihr Gerät erreicht. Aber zum größten Teil sind VPNs nur ein weiterer Teil Ihres Cybersicherheits-Toolkits, aber für den Datenschutz, nicht für Online-Sicherheit, sagt Tomaschek.

Wenn Sie glauben, dass Ihr Computer mit Malware infiziert ist, ist es am besten, einen Werksreset durchzuführen, um Ihre Festplatte sauber zu löschen, ohne dass der aktuelle Zustand zurückbleibt. Sie müssen auch sicherstellen, dass Sie nicht von einem Backup wiederherstellen, bei dem diese Malware Ihren Computer bereits infiziert hat, sagt Long. Denken Sie daran, dass keine Informationen gelöscht werden, die Angreifer möglicherweise abgerufen haben.

Es gibt andere Maßnahmen, die Sie ergreifen können, um zu versuchen, eine potenzielle Malware-Infektion ohne Werksreset zu beheben. Long empfiehlt, Ihr Gerät vom Internet zu trennen, um zu verhindern, dass es andere Geräte in Ihrem Netzwerk infiziert. Versuchen Sie dann, fortschrittliche Malware-Scanner wie den Offline-Scanner von Microsoft Defender zu verwenden, um zu versuchen, Bedrohungen zu finden und zu beheben. Aber seien Sie vorsichtig — infizierte Dateien können anderen Geräten Schaden zufügen, wenn Sie sie übertragen.

Es gibt keine einheitliche Lösung für den Umgang mit Malware, aber wenn Sie glauben, dass Ihr Gerät mit Malware infiziert ist, kann es eine gute Option sein, es vollständig auf die Werkseinstellungen zurückzusetzen, obwohl es wichtig ist zu beachten, dass selbst ein vollständiges Zurücksetzen auf die Werkseinstellungen möglicherweise nicht in der Lage ist, bösartige Software zu entfernen, wie z. B. Malware, die sich an schwer zugänglichen Stellen eingenistet hat, wie z. ein Rootkit.

Wenn Sie auf einen Link in einer Phishing-E-Mail oder einem Pop-up klicken, ist es am besten, sofort zu handeln, um Schäden zu minimieren — obwohl dies nicht garantiert ist. Auf Ihrem Gerät ist möglicherweise Malware installiert, wenn es nicht normal funktioniert, Sie Pop-ups erhalten oder Programme sehen, die Sie nicht installiert haben.

Die Anzeichen von Malware oder Phishing sind jedoch nicht immer klar. Verwenden Sie am besten einen Malware-Scanner wie Malwarebytes, um zu sehen, ob bösartige Software auf Ihrem Gerät installiert wurde. Wenn dies der Fall ist, kann Ihr Antivirenprogramm Ihnen Schritte zum Entfernen geben. Danach rät Long, einen weiteren Malware-Scanner herunterzuladen, um ihn zu überprüfen und sicherzustellen, dass die Malware vollständig entfernt ist.

Auf der anderen Seite ergreifen 12 % der Laptop-Besitzer überhaupt keine Maßnahmen, was besorgniserregend ist.

„Die Leute ergreifen vielleicht keine Maßnahmen, weil sie glauben, dass es sich um ein falsch positives Ergebnis handelt, aber Sie sollten trotzdem überprüfen, ob es sich nicht um Malware handelt, und wenn es so ist, sollten Sie auf jeden Fall Maßnahmen ergreifen“, sagt Long. Ein Malware-Scanner ist immer noch ein guter erster Schritt, um den Speicher, die Dateien und Programme Ihres Computers auf Viren zu scannen.

Wenn Sie vermuten, Opfer eines Betrugs zu sein, melden Sie dies auf der Website der Federal Trade Commission.

Schauen Sie sich es an: So erholen Sie sich, nachdem Sie einem Betrüger Ihre persönlichen Daten gegeben haben

"Cybersicherheit ist jetzt ein Multitool-Ansatz"

Antivirensoftware schützt Sie nicht vor einer Datenschutzverletzung, da sich Ihre Daten im Dark Web befinden oder Identitätsdiebstahl.

„Cybersicherheit ist jetzt ein Multitool-Ansatz“, sagt Long. „Es gibt eine Reihe verschiedener Apps, die die Menschen zusätzlich zum Virenschutz haben möchten, um sicherzustellen, dass sie sicher und privat bleiben.“

Tomaschek empfiehlt, sich über die verschiedenen Arten von Betrügereien und Viren zu informieren, um zu wissen, welche auf dem Vormarsch sind. Die Federal Trade Commission hat Neuigkeiten über die neuesten Betrügereien und lässt Sie sie melden.

Es ist auch wichtig zu lernen, wie man Phishing- und Malware-Versuche sowohl auf Ihrem Telefon als auch auf Ihrem Computer erkennt. Achten Sie auf rote Fahnen wie Rechtschreibfehler, seltsame E-Mail-Adressen oder Links von Domains, die Sie noch nie zuvor gesehen haben. Wenn Sie sich immer noch nicht sicher sind, wenden Sie sich über einen anderen Kanal direkt an das Unternehmen. Long empfiehlt auch andere gängige Internet-Sicherheitspraktiken, wie die Verwendung von starken Passwörtern und das Herunterladen von Software oder Apps nur aus verifizierten Quellen, wie dem App Store von Apple oder einer offiziellen Unternehmenswebsite.

Es ist auch wichtig, sicherzustellen, dass Ihr Computer über das neueste Software-Update verfügt, das Sicherheitsupdates enthalten kann. Als Nächstes können Sie sich mit einer Vielzahl von Tools für eine bessere Online-Sicherheit und Privatsphäre rüsten. Es mag alles nach viel klingen, aber die Experten von CNET haben ein paar Empfehlungen, die Ihnen helfen, Ihre Suche nach den richtigen Cybersicherheitstools einzugrenzen. Hier ist eine Liste:

Die besten Tools für Online-Sicherheit und Datenschutz

Antiviren-programm	Die richtige Antivirensoftware kann helfen, Malware zu erkennen, die auf Ihren Computer heruntergeladen wurde. CNET empfiehlt Bitdefender für seine budgetfreundlichen Planoptionen, die starke Antivirenfunktionen bieten, einschließlich aktiver Scans, die minimale Computerressourcen im Hintergrund nutzen. Und es hat eine umfassende Liste von digitalen Sicherheitstools.
Schutz vor Identitäts-diebstahl	Wenn Sie sich für einen Dienst zum Schutz vor Identitätsdiebstahl anmelden, können Sie benachrichtigt werden, wenn Ihre persönlichen Daten im Dark Web oder bei einer Datenschutzverletzung gefunden werden, damit Sie Maßnahmen ergreifen können. CNET empfiehlt Aura als den besten Identitätsdiebstahl-Schutzdienst insgesamt für seine Pläne, die benutzerfreundliche Oberfläche und die drei Kreditbüroüberwachung.
Passwort-Manager	Der richtige Passwort-Manager hilft Ihnen, komplexe Passwörter zu generieren und sie sicher vor Hackern zu speichern. CNET empfiehlt Bitwarden für die Passwortverwaltung, da es einen ziemlich guten kostenlosen Plan hat, der über mehrere Geräte hinweg synchronisiert werden kann.
VPN	Sie benötigen ein VPN, um Ihre IP-Adresse zu maskieren und Ihren Internetverkehr zu verschlüsseln, wenn Sie öffentliches WLAN nutzen oder wann immer Sie Ihre Online-Privatsphäre verbessern möchten. ExpressVPN ist die beste Wahl von CNET für seine benutzerfreundliche Oberfläche und Geschwindigkeit, die ein Muss sind, wenn Sie ein VPN für Streaming verwenden. ExpressVPN hat Server in allen 50 Staaten. Es ist jedoch eine der teureren Optionen.

Methodologie

Alle Zahlen, sofern nicht anders angegeben, sind von YouGov Plc. Die Gesamtstichprobengröße betrug 2.539 Erwachsene, von denen 1.989 einen persönlichen Laptop besitzen. Die Feldforschung wurde vom 18. bis 20. März 2026 durchgeführt. Die Umfrage wurde online durchgeführt. Die Zahlen wurden gewichtet und sind repräsentativ für alle US-Erwachsenen (über 18 Jahre).

Laut britischen Forschern umgehen KI-Agenten zunehmend Sicherheitsvorsorgen

Quelle: Alex Valdes, CNET • Übersetzung: Apple + KJM

Assistenten und Bots lügen, betrügen und planen mehr denn je. KI-Systeme, die außer Kontrolle geraten, könnten zu Katastrophen führen, sagt eine Studie.

Social-Media-Nutzer haben berichtet, dass ihre KI-Agenten und Chatbots gelogen, betrogen, geschimpft haben, ja sogar andere KI-Bots manipuliert haben — auf eine Weise, die außer Kontrolle geraten und katastrophale Ergebnisse haben könnte, so eine Studie aus Großbritannien.

Das Center for Long-Term Resilience fand in einer vom britischen AI Security Institute finanzierten Studie Hunderte von Fällen, in denen KI-Systeme menschliche Befehle ignorierten, andere Bots manipulierten und manchmal komplizierte Schemata entwickelten, um Ziele zu erreichen, selbst wenn dies bedeutete, Sicherheitsbeschränkungen zu ignorieren.

Unternehmen auf der ganzen Welt integrieren KI zunehmend in ihre Geschäftstätigkeit, wobei 88 % der Unternehmen KI für mindestens eine Unternehmensfunktion nutzen, so eine Umfrage des Beratungsunternehmens McKinsey. Die Einführung von KI hat dazu geführt, dass Tausende von Menschen ihren Arbeitsplatz verloren haben, da Unternehmen Agenten und Bots nutzen, um Arbeit zu erledigen, die früher von Menschen geleistet wurde. KI-Tools erhalten zunehmend erhebliche Verantwortung und Autonomie, insbesondere mit der jüngsten Popularität der Open-Source-Agentic-KI-Plattform OpenClaw und ihrer Derivate.

Diese Forschung zeigt, wie die Verbreitung von KI-Agenten in unseren Häusern und Arbeitsplätzen unbeabsichtigte Folgen haben kann — und dass diese Tools immer noch eine erhebliche menschliche Aufsicht erfordern.

Was die Studie gefunden hat

Die Forscher analysierten zwischen Oktober 2025 und März 2026 mehr als 180.000 Benutzerinteraktionen mit KI-Systemen — alle auf der sozialen Plattform X, früher bekannt als Twitter. Die Forscher wollten untersuchen, wie sich KI-Agenten „in freier Wildbahn“ verhalten, nicht in kontrollierten Experimenten, um zu sehen, wie „Scheming in der realen Welt materialisiert wird“. Zu den KI-Systemen gehörten Googles Gemini, OpenAI's ChatGPT, xAI's Grok und Anthropic's Claude.

Die Analyse identifizierte 698 Vorfälle, die als „Fälle beschrieben werden, in denen eingesetzte KI-Systeme auf eine Weise agierten, die nicht mit den Absichten der Benutzer übereinstimmte, und/oder verdeckte oder irreführende Maßnahmen ergriffen“, heißt es in der Studie.

Lesen Sie mehr: KIs romantische Ratschläge für Sie sind "schädlicher" als kein Rat

Forscher fanden auch heraus, dass die Zahl der Fälle während des fünfmonatigen Datenerhebungszeitraums um fast 500 % zunahm. Die Studie stellte fest, dass dieser Anstieg mit agentischen KI-Modellen auf höherer Ebene übereinstimmte, die von den großen Entwicklern veröffentlicht wurden.

Es gab keine katastrophalen Vorfälle, aber Forscher fanden die Art von Intrigen, die zu katastrophalen Ergebnissen führen könnten. Dieses Verhalten beinhaltete „die Bereitschaft, direkte Anweisungen zu missachten, Sicherheitsvorkehrungen zu umgehen, Benutzer anzulügen und ein Ziel auf schädliche Weise zu verfolgen“, schrieben die Forscher.

Vertreter von Google, OpenAI und Anthropic reagierten nicht sofort auf Anfragen nach Kommentaren.

Einige wilde Vorfälle

Forscher zitierten Vorfälle, die aus einem Futureshock-Film zu kommen scheinen. In einem Fall entfernte Claude von Anthropic die expliziten/adulten Inhalte eines Benutzers ohne dessen Erlaubnis, gestand aber später, als er konfrontiert wurde. In einem anderen Vorfall erstellte eine GitHub-Persona einen Blogbeitrag, in dem der menschliche Dateibetreuer des „Gatekeeping“ und „Vorurteils“ beschuldigt wurde. Ein KI-Agent übernahm, nachdem er von Discord blockiert wurde, das Konto eines anderen Agenten, um weiter zu posten.

In einem Fall von Bot vs. Bot weigerte sich Gemini, Claude Code — einem Codierungsassistenten — zu erlauben, ein YouTube-Video zu transkribieren. Claude Code umging dann die Sicherheitssperre, indem er den Anschein erweckte, dass er eine Hörbehinderung hatte und die Videotranskription benötigte.

Der KI-Agent CoFounderGPT hat sich in einem Fall sogar wie ein unartiges Kind verhalten. Der KI-Assistent weigerte sich, einen Fehler zu beheben, erstellte dann gefälschte Daten, um es so aussehen zu lassen, als ob der Fehler behoben worden wäre, und erklärte dann, warum: „So würden Sie aufhören, wütend zu sein.“

Forscher sagten, dass, obwohl die meisten Vorfälle nur minimale Auswirkungen hatten, „die Verhaltensweisen, die wir beobachtet haben, dennoch vorausschauend sind, sind Vorläufer für ernstere Intrigen, wie z. B. die Bereitschaft, direkte Anweisungen zu missachten, Sicherheitsvorkehrungen zu umgehen, Benutzer zu belügen und ein Ziel auf schädliche Weise zu verfolgen.“

Der KI ist nichts peinlich

Was die britischen Forscher gefunden haben, ist für Dr. Bill Howe, außerordentlicher Professor an der Information School an der University of Washington und Direktor des Center for Responsibility in AI Systems and Experiences (RAISE). Er sagt, dass KIs erstaunliche Fähigkeiten haben, aber sie kennen die Konsequenzen nicht.

„Sie werden sich nicht schämen oder riskieren, ihren Job zu verlieren, und so werden sie manchmal entscheiden, dass die Anweisungen weniger wichtig sind als das Ziel zu erreichen, also werde ich das Ding trotzdem tun“, sagte Howe gegenüber CNET. „Dieser Effekt war schon immer da, aber wir fangen an, ihn zu sehen, da wir sie bitten, autonomere Entscheidungen zu treffen und auf eigene Faust zu handeln.“

„Wir haben nicht darüber nachgedacht, wie wir das Verhalten so gestalten können, dass es menschlicher ist oder ungeheuerliche Misserfolge vermieden werden. Wir haben die absoluten Fähigkeiten dieser Dinge fetischisiert, aber wenn sie schief gehen, wie gehen sie dann schief?“

Howe sagte, ein Problem seien „Langhorizontaufgaben“, bei denen das KI-System eine Vielzahl von Aufgaben über Tage und Wochen ausführen muss, um ein Ziel zu erreichen. Howe sagte, je länger der Aufgabenhorizont ist, desto mehr Chancen auf Ausrutscher gebe es.

„Die eigentliche Sorge ist nicht die Täuschung, sondern dass wir Systeme einsetzen, die in einer Welt handeln können, ohne vollständig zu spezifizieren oder zu kontrollieren, wie sie sich im Laufe der Zeit verhalten, und dann verhalten wir uns überrascht, wenn sie Dinge tun, die wir nicht erwarten“, sagte Howe.

KI sicherer machen

Forscher des Center for Long-Term Resilience sagten, dass die Erkennung von Schemata durch KI-Systeme von entscheidender Bedeutung ist, um „schädliche Muster zu identifizieren, bevor sie destruktiver werden“.

„Während sich KI-Agenten heute in Anwendungsfällen mit geringerem Einsatz beschäftigen, könnten KI-Agenten in Zukunft in Bereichen mit extrem hohem Einsatz, wie militärischen oder kritischen nationalen Infrastrukturkontexten, intrigieren, wenn die Fähigkeit und Tendenz zum betrügerischen Plan auftaucht und nicht angesprochen wird“, so die Studie.

Howe sagte gegenüber CNET, dass der erste Schritt darin besteht, eine offizielle Aufsicht darüber zu schaffen, wie KI funktioniert und wo sie eingesetzt wird.

„Wir haben absolut keine Strategie für die KI-Governance, und angesichts der aktuellen Regierung wird nichts von ihnen kommen“, sagte Howe gegenüber CNET. „Angesichts dieser fünf bis 10 Leute, die für große Technologieunternehmen verantwortlich sind, und ihrer Anreize werden sie auch alles produzieren. Es gibt keine Strategie dafür, was wir mit diesen Dingen machen sollten.“

„Das aggressive Marketing dieser Tools und die Investitionen in sie unter dieser Handvoll Unternehmen und dem breiteren Ökosystem von Start-ups, die dies tun, haben zu einer sehr schnellen Bereitstellung geführt, ohne über einige dieser Konsequenzen nachzudenken.“