Apple: Langlebigkeit durch Design

Howard Oakley, exlecticlight.co • Übersetzung: KJM

Obwohl die meisten von uns, die Macs verwenden, anerkennen, dass diese in der Regel länger halten als die Produkte der meisten Konkurrenten, haben wir auch gemeinsame Bedenken hinsichtlich ihrer Langlebigkeit. macOS-Upgrades und -Updates mögen zwar kostenlos sein, aber sie sind auch zeitlich begrenzt, so dass jede Version nur ein Jahr lang vollständig unterstützt wird und dann für weitere zwei Jahre mit Sicherheitsupdates versorgt wird. Es gibt auch Bedenken in Bezug auf die Aufrüstbarkeit, da die meisten modernen Macs vom Tag der Herstellung bis zur Entsorgung mit demselben Arbeitsspeicher und internen Speicher ausgestattet sind. Einige sind der Meinung, dass dies zu einer eingebauten Obsoleszenz führe.

Apple hat sein langes Schweigen zu diesem Thema kürzlich gebrochen, und zwar in einem White Paper mit dem Titel „Longevity by Design“, in dem es vor allem mit iPhones argumentiert, von denen es nach eigenen Angaben inzwischen „Hunderte von Millionen“ gibt, die seit mehr als fünf Jahren in Gebrauch sind. Obwohl ich vermute, dass die Schätzungen für ältere Macs weniger präzise sind, ist es eine Schande, dass dazu keine vergleichbaren Zahlen genannt werden.

In vielerlei Hinsicht liefert Apple ein überzeugendes Argument, wie das Beispiel des Eindringens von Flüssigkeiten in iPhones zeigt. Frühe Modelle boten nur wenig Schutz, und Reparaturen aufgrund von eingedrungener Flüssigkeit waren an der Tagesordnung. Die Apple-Ingenieure machten sich daran, iPhones widerstandsfähig zu machen, entwickelten Lösungen mit veränderten Komponenten, Dichtungen und mehr und testeten sie ausgiebig. Das iPhone 7 und 7 Plus waren die ersten Modelle, die einen vollständigen Schutz gegen das Eindringen von Flüssigkeiten aufwiesen, was zu einem Rückgang der Reparaturen aufgrund von Flüssigkeitsschäden um 75 % führte. Dieser Schutz hat nach wie vor hohe Priorität bei der Entwicklung und den Tests von iPhones; seltsamerweise wurden keine vergleichbaren Anstrengungen zum Schutz von iPads unternommen.

Die Schwachstelle von Apple ist die macOS-Unterstützung. Obwohl das White Paper feststellt, dass „eine der wichtigsten Säulen für die Langlebigkeit von Produkten der Software-Support ist, insbesondere Sicherheitsupdates und Fehlerbehebungen“, vermeidet es, Apples macOS-Support-Politik von 1 + 2 Jahren zu erwähnen. Das ist seltsam, da diese Politik zwar bekannt ist, aber (soweit ich weiß) nie schriftlich formuliert wurde.

In dem Papier wird dann kühn behauptet, dass „macOS Sonoma mit Mac-Computern kompatibel ist, die 2017 eingeführt wurden. Aber auch nachdem ein Apple-Produkt nicht mehr mit dem neuesten Apple-Betriebssystem aktualisiert werden kann, bemühen wir uns, unsere Kunden mit kritischen Sicherheitsupdates zu versorgen“.

Was nicht gesagt wird, ist, dass der einzige Mac aus dem Jahr 2017, der noch von Sonoma unterstützt wird, der iMac Pro ist, das damalige Spitzenmodell, und der einzige Mac, der in diesem Jahr veröffentlicht wurde und von Sequoia unterstützt wird. Die Situation wird sich diesen Herbst mit macOS 15 ändern, das die Unterstützung für zwei neuere MacBook Air Modelle einstellt.

Apples Pionierarbeit im Bereich der Reparierbarkeit ist stark unterbewertet. Der Macintosh II aus dem Jahr 1987 war einer der ersten Personalcomputer mit modularem Design, so dass Händler nicht mit dem Lötkolben hantieren mussten, um Hardwareprobleme zu beheben. Stattdessen tauschten ihre Servicetechniker eine modulare Komponente, z. B. ein Netzteil, aus und schickten das defekte Modul zur Prüfung und eventuellen Wiederaufbereitung an Apple zurück.

Es gibt wertvolle Einblicke, wie Apple die Reparatur seiner Produkte verändert und in den letzten fünf Jahren die Größe seines Service- und Reparaturnetzes verdoppelt hat. Das Ergebnis ist beeindruckend: Es wird behauptet, dass 85 % der US-Bevölkerung in einem Umkreis von 30 Minuten um einen Apple Store, einen Apple Authorized Service Provider (AASP) oder einen Independent Repair Provider (IRP) zu finden sind. Im Vereinigten Königreich trifft das auf 82 % der Bevölkerung zu, in Italien und Deutschland sind es 89 %."

Es gibt seit langem Gerüchte darüber, dass Apple die Lieferung von Teilen, Werkzeugen oder Reparaturdiensten durch Drittanbieter erschwert. Einige Hersteller erreichen dies unter anderem dadurch, dass sie ihre Garantien aufheben, wenn Dritte beteiligt waren. Apple stellt seine Politik klar: „Die Apple-Garantie wird durch eine Reparatur außerhalb des von Apple autorisierten Netzwerks oder durch die Verwendung von Teilen oder Werkzeugen von Drittanbietern nicht beeinträchtigt, es sei denn, das Produkt wird im Verlauf der Reparatur beschädigt. Wir werden keine Teile von Drittanbietern, die nach denselben Spezifikationen wie unsere Produkte hergestellt werden, aktiv deaktivieren, es sei denn, sie beeinträchtigen die Sicherheit und den Datenschutz des Kunden, was derzeit auf biometrische Teile beschränkt ist."

Letzteres wird in dem Papier später klargestellt: „Es gibt nur ein Szenario, in dem Apple ein Teil eines Drittanbieters deaktivieren wird: wenn ein Face ID- oder Touch ID-Sensor eines Drittanbieters installiert wird, werden wir die Authentifizierung deaktivieren, um Sicherheit und Datenschutz zu gewährleisten."

Sie sollten eine Kopie dieses Whitepapers aufbewahren, für den Fall, dass Sie jemals die Apple-Richtlinien überprüfen müssen.

Es gibt wichtige Einblicke in einen bisher undurchsichtigen Bereich: Service/Reparatur und die Privatsphäre von Daten auf einem Mac oder Gerät. Seit 2018 verwendet Apple eine Reihe von Software-Tools zur Ferndiagnose von Hardware-Problemen, ohne dass Servicetechniker nach Passwörtern oder Passcodes fragen müssen, um so Zugriff auf Ihre verschlüsselten Daten auf einem kranken Mac oder Gerät zu erhalten.

Schließlich gibt Apple Details zu zwei wichtigen Änderungen, zumindest für iPhones. Die erste ist die Hinzufügung eines Abschnitts „Teile- und Wartungsverlauf" in "Einstellungen" > „Allgemein" > „Info" für alle Geräte, an denen eine wichtige Komponente repariert wurde. Wurden Originalteile von Apple verwendet, wird dies dort vermerkt und informiert künftige Besitzer über die Herkunft der Komponenten des iPhones. Dies ist natürlich ein guter Weg, um die Besitzer zu ermutigen, ihre iPhones durch das autorisierte Apple-Netzwerk mit offiziellen Apple-Teilen reparieren zu lassen.

Der andere Blick in die Zukunft betrifft die Aktivierungssperre für das iPhone, die in Zukunft einzelne Teile abdecken wird, um den Diebstahl des Geräts zu verhindern. „Wenn ein Gerät während einer Reparatur feststellt, dass ein unterstütztes Teil von einem anderen iPhone mit aktivierter Aktivierungssperre oder aktiviertem Verlustmodus stammt, schränken wir die Kalibrierung für dieses Teil ein", was in der Teile- und Service-Historie vermerkt wird.

Obwohl Apple keineswegs perfekt ist, macht dieses White Paper deutlich, dass Apple sich um die Langlebigkeit seiner Produkte kümmert, und zwar mehr als seine Konkurrenten. Es endet auch mit einer ausdrücklichen und nachdrücklichen Verneinung der Idee der eingebauten Obsoleszenz.

Apple warnt vor neuem Scam und nennt Tipps, um sich zu schützen

Quelle: bk, mactechnews.de

Es gibt mehrere Möglichkeiten, sich unberechtigten Zugang zu Nutzer-Accounts zu verschaffen: Neben Brute-Force-Angriffen, die vor allem bei eher simplen Passwörtern ein überaus wirkungsvolles Instrument darstellen, lassen sich viele auch mit mehr oder minder ausgefeilten Social-Engineering-Strategien überlisten. Natürlich wecken auch Apple-IDs das Interesse von Angreifern: In den USA sind gerade fingierte SMS-Textnachrichten im Umlauf, in denen eine wichtige Anfrage von Apple vorgegaukelt wird. Nutzer sollen auf einen Link in der Mitteilung klicken, weiterhin von iCloud Gebrauch machen zu können. Die Masche dürfte sich wohl bald auf andere Länder ausstrecken. Cupertino reagiert auf Vorfälle dieser Art mit einem aktualisierten Support-Dokument.

Apple schlüsselt Angriffsmethoden auf

Apple geht eingehend darauf ein, mit welchen Methoden und betrügerischen Absichten Angreifer vorgehen und wie sich Anwender am besten schützen. Manche der Tipps sind auch bei anderen Accounts hilfreich: So rät der Konzern dazu, auf keine Links in verdächtigen Nachrichten zu klicken und Sicherheitsinformationen wie Passwörter nicht weiterzugeben. Ferner empfiehlt Apple die Einrichtung einer Zwei-Faktor-Authentifizierung. Geschenkkarten sollten außerdem nicht dazu benutzt werden, um jemanden zu bezahlen — für dieses Phänomen liegt sogar eine gesonderte Seite vor. Der Bezug von Software erfolgt am besten lediglich über vertrauenswürdige Quellen. Vorsicht ist zudem bei der Installation womöglich unerwünschter Konfigurationsprofile sowie bei Pop-up-Fenstern im Browser geboten. Apple betont, niemals die Deaktivierung von Sicherheitsfunktionen auf dem Gerät oder für die Apple-ID zu fordern.

SMS und Mails bei Apple melden

Sollten Nutzer SMS oder E-Mails erhalten, welche nicht von Apple sind, aber deren Aufmachung an das Unternehmen erinnert, so rät Cupertino zur Weiterleitung an reportphishing@apple.com. Bei verdächtigen FaceTime-Anrufen können Nutzer Screenshots mit den Informationen erstellen und sie an reportfacetimefraud@apple.com schicken. Bei Anrufen, welche nur scheinbar von Apple kommen, ist der Ratschlag ein besonders schlichter, wenngleich wirkungsvoller: Der Angerufene soll einfach auflegen. Apple ruft ohnehin nicht grundlos Nutzer an.

Apple erklärt, wie man Social-Engineering-Angriffe erkennen kann

Adam Engst, tidbits.com • Übersetzung KJM

In einem bemerkenswerten Update eines Support-Dokuments, das erklärt, wie man Betrügereien erkennen und vermeiden kann, schreibt Apple:

Social Engineering ist eine Art von gezielten Angriffen, die auf Imitation, Täuschung und Manipulation beruhen, um Zugang zu Ihren persönlichen Daten zu erhalten. Bei diesem Angriff geben sich die Betrüger am Telefon oder über andere Kommunikationsmethoden als Vertreter eines vertrauenswürdigen Unternehmens oder einer Einrichtung aus. Sie wenden oft ausgeklügelte Taktiken an, um Sie dazu zu bringen, persönliche Daten wie Anmeldedaten, Sicherheitscodes und Finanzinformationen preiszugeben.

Das Dokument, das erstmals Ende 2023 in der Wayback Machine auftauchte, enthält nichts, was sicherheitsbewusste Apple-Benutzer überraschen würde, aber es ist eine hervorragende Zusammenfassung, die Sie an diejenigen weitergeben können, die weniger über Betrügereien im technischen Bereich informiert sind.

Sie enthält auch alle E-Mail-Adressen, an die Sie Betrüger melden können, die sich als Apple ausgeben. Das Update vom 4. Juli 2024 enthält einen besonders hilfreichen Abschnitt zur Erkennung von Social-Engineering-Angriffen aller Art.

Hier folgt der originale Artikel von Apples Support-Seiten:

Social-Engineering-Schemata wie Phishing-Nachrichten, gefälschte Support-Anrufe und andere Betrugsversuche erkennen und vermeiden

Apple Support • Veröffentlichungsdatum: 04. Juli 2024

Mit diesen Tipps kannst du dich vor Betrugsversuchen schützen, und du erfährst, was zu tun ist, wenn du verdächtige E-Mails, Anrufe oder sonstige Nachrichten bekommst.

Social Engineering ist ein gezielter Angriff, der auf Identitätsdiebstahl, Täuschung und Manipulation beruht, um Zugriff auf deine persönlichen Daten zu erlangen. Bei diesem Angriff geben sich Betrüger telefonisch oder über andere Kommunikationsmethoden als Vertreter eines vertrauenswürdigen Unternehmens oder einer vertrauenswürdigen Einrichtung aus. Häufig wenden sie raffinierte Praktiken an, um dich dazu zu überreden, persönliche Daten wie Anmeldedaten, Sicherheitscodes und Finanzdaten preiszugeben.

Phishing ist eine gängige Methode des Social Engineering, die sich auf betrügerische Versuche bezieht, an persönliche Daten zu gelangen (üblicherweise per E-Mail). Betrüger setzen jedoch alle Mittel ein, um dich dazu zu bringen, Informationen preiszugeben oder ihnen Geld zu geben, darunter:

- Betrügerische E-Mails und andere Nachrichten, die aussehen, als stammten sie von legitimen Unternehmen wie Apple.
- Irreführende Popups und Anzeigen, die besagen, dass dein Gerät ein Sicherheitsproblem hat.
- Betrügerische Telefonanrufe oder Voicemails, die sich als Apple Support, Apple Partner und andere bekannte oder vertrauenswürdige Organisationen oder Einzelpersonen ausgeben.
- Gefälschte Werbeaktionen, die kostenlose Produkte und Preise anbieten.
- Unerwünschte Kalendereinladungen und Abonnements.

Wenn du einen Verdacht bezüglich einer Nachricht, eines Anrufs oder einer Anfrage zur Angabe persönlicher Daten wie E-Mail-Adresse, Telefonnummer, Passwort, Sicherheitscode oder einem Geldbetrag hast, ist es sicherer, davon auszugehen, dass es sich um Betrug handelt. Wende dich gegebenenfalls direkt an das Unternehmen.

Wenn du Bedenken hinsichtlich eines Sicherheitsproblems mit deinem Apple-Gerät oder -Account hast, bieten diese Ressourcen weitere Informationen, die dir weiterhelfen können.

Wenn du glaubst, dass deine Apple-ID gefährdet ist, oder wenn du dein Passwort oder andere persönliche Daten auf einer betrügerischen Website eingegeben hast, ändere dein Apple-ID Passwort sofort, und vergewissere dich, dass die Zwei-Faktor-Authentifizierung aktiviert ist.

Apple-Account und -Geräte schützen

Hier ein paar Tipps, wie du dich gegen Betrugsversuche schützen kannst, die auf Apple-Accounts und -Geräte abzielen.

- Gib niemals persönliche Daten oder Sicherheitsinformationen wie Passwörter oder Sicherheitscodes weiter, und stimme deren Eingabe niemals auf einer Webseite zu, auf die dich jemand weiterleitet.
- Schütze deine Apple-ID: Verwende die Zwei-Faktor-Authentifizierung. Bewahre deine Kontaktinformationen sicher auf und halte sie auf dem neuesten Stand. Gib dein Apple-ID-Passwort oder deinen Bestätigungscode niemals an Dritte weiter. Apple fragt diese Angaben für den Support niemals ab.
- Verwende niemals Apple-Gift Cards, um jemanden zu bezahlen.
- Informiere dich, wie du seriöse E-Mails von Apple zu deinen App Store- oder iTunes Store-Käufen erkennst. Wenn du mit Apple Cash Geld sendest oder empfängst (nur USA), behandle es wie jede andere private Transaktion.
- Informiere dich, wie du deine Apple-Geräte und Daten schützt.
- Lade Software nur von vertrauenswürdigen Quellen.
- Klicke nie auf Links in verdächtigen oder unaufgefordert erhaltenen Nachrichten, und öffne bzw. lade keine Anhänge solcher Nachrichten.
- Beantworte keine verdächtigen Anrufe oder Nachrichten, die angeblich von Apple stammen. Kontaktiere Apple stattdessen direkt über unsere offiziellen Supportkanäle.

Verdächtige E-Mails, Nachrichten und Anrufe melden

- Wenn du eine verdächtige E-Mail erhältst, die anscheinend von Apple stammt, leite sie bitte weiter an reportphishing@apple.com.[1]
- Wenn du einen verdächtigen FaceTime-Anruf erhältst (z. B. vermeintlich von einer Bank oder einem Finanzinstitut), sende ein Bildschirmfoto der Anrufinformationen per E-Mail an reportfacetimefraud@apple.com. Um die Anrufinformationen zu erhalten, öffne FaceTime, und tippe auf die Info-Taste ⓘ neben dem verdächtigen Anruf.
- Wenn du in der Nachrichten- oder Mail-App einen verdächtigen Link zu einem FaceTime-Anruf erhält, sende ein Bildschirmfoto des Links per E-Mail an reportfacetimefraud@apple.com. Das Bildschirmfoto sollte die Telefonnummer oder E-Mail-Adresse enthalten, über die der Link gesendet wurde.
- Um eine verdächtige SMS zu melden, die scheinbar von Apple stammt, nimm ein Bildschirmfoto der Nachricht auf, und sende das Bildschirmfoto per E-Mail an reportphishing@apple.com.
- Um Spam zu melden, den du in deinem Posteingang von iCloud.com, me.com oder mac.com erhältst, markiere die Spam-E-Mails als Spam, oder verschiebe sie in deinen iCloud-Spam-Ordner. Wenn du eine E-Mail als Spam markierst, verbesserst du die iCloud-Mail-Filterung und reduzierst zukünftigen Spam.
- Um Belästigungen, Identitätsbetrugsversuche und andere Fälle von Missbrauch zu melden, die du in deinem Posteingang von iCloud.com, me.com oder mac.com erhältst, sende sie an abuse@icloud.com.
- Um Spam oder andere verdächtige Nachrichten zu melden, die du über „Nachrichten“ erhältst, tippe unter der Nachricht auf „Spam melden“. Du kannst unerwünschte Nachrichten und Anrufe auch blockieren.
- Melde betrügerische Anrufe bei der Federal Trade Commission (nur USA) unter reportfraud.ftc.gov, oder wende dich an deine örtliche Strafverfolgungsbehörde.

Weitere Infos zu Social-Engineering-Angriffen, Phishing und anderen Betrugsversuchen

Hier erfährst du, wie du Social Engineering-Angriffe und Phishing-Nachrichten erkennst, auf betrügerische Anrufe reagierst und andere Online-Betrugsversuche vermeidest.

Social-Engineering-Angreifer nutzen Identitätswechsel und Manipulation, um zunächst dein Vertrauen zu gewinnen. Dann verleiten sie dich dazu, vertrauliche Daten herauszugeben oder ihnen Zugriff auf deine Accountinformationen zu gewähren. Sie wenden eine Vielzahl von Praktiken an, um sich als vertrauenswürdiges Unternehmen, eine vertrauenswürdige Rechtspersönlichkeit oder eine dir bekannte Person auszugeben.

Achte auf diese Anzeichen, um festzustellen, ob du im Rahmen eines Social-Engineering-Angriffs anvisiert wirst:

- Ein Betrüger kann dich von einer scheinbar legitimen Telefonnummer von Apple oder einem anderen vertrauenswürdigen Unternehmen aus anrufen. Dies wird als „Spoofing“ bezeichnet.” Wenn der Anruf verdächtig erscheint, kannst du auflegen und die geprüfte Nummer des Unternehmens selbst wählen.
- Betrüger erwähnen oft persönliche Informationen über dich, um Vertrauen aufzubauen, und als legitimiert zu erscheinen. Dabei kann es sich um Informationen handeln, die du als privat ansiehst, z. B. deine Privatadresse, deinen Arbeitsplatz oder sogar deine Sozialversicherungsnummer.
- Oftmals vermitteln sie den Wunsch, dir bei der Lösung eines unmittelbaren Problems zu helfen. Beispielsweise wird behauptet, dass jemand in deinen iPhone- oder iCloud-Account eingedrungen ist oder über Apple Pay nicht autorisierte Zahlungen vorgenommen hat. Der Betrüger gibt an, dir helfen zu wollen, die Angreifer aufzuhalten oder die Zahlungen rückgängig zu machen.
- Der Betrüger erzeugt normalerweise ein starkes Gefühl der Dringlichkeit, um dir keine Zeit zum Nachdenken zu geben, und um dich davon abzuhalten, dich direkt an Apple zu wenden. Der Betrüger kann beispielsweise sagen, dass es dir zwar freisteht, dich direkt an Apple zu wenden, aber in der Zeit würden die betrügerischen Aktivitäten fortgesetzt werden und du müsstest dafür haften. Dies ist falsch und soll lediglich verhindern, dass du sofort auflegst.
- Schließlich wollen Betrüger deine Account-Informationen oder Sicherheitscodes wissen. In der Regel wirst du auf eine gefälschte Website weitergeleitet, die wie eine echte Apple-Anmeldeseite aussieht, und aufgefordert, deine Identität zu verifizieren. Apple wird dich niemals auffordern, dich bei einer Website anzumelden oder im Dialogfeld für die Zwei-Faktor-Authentifizierung auf „Akzeptieren“ zu

[1] Um eine SMS zu melden, nimm ein Bildschirmfoto der Nachricht auf, und sende es per E-Mail. Wenn du über Mail auf deinem Mac eine Nachricht weiterleitest, füge die Header-Informationen hinzu. Wähle dazu die Nachricht aus, und wähle im Menü „Nachricht“ die Option „Als Anhang weiterleiten“.

tippen oder dein Passwort, deinen Gerätecode oder deinen Code für die Zwei-Faktor-Authentifizierung auf einer Website einzugeben.

- Eventuell fordern dich die Betrüger auf, Sicherheitsfunktionen wie die Zwei-Faktor-Authentifizierung oder den Schutz für gestohlene Geräte zu deaktivieren. Sie behaupten, dass dies notwendig ist, um einen Angriff abzuwehren oder um dir zu ermöglichen, die Kontrolle über deinen Account zurückzuerlangen. Sie versuchen damit, dich dazu zu verleiten, deine Sicherheit zu verringern, damit sie ihren eigenen Angriff ausführen können. Apple wird dich niemals dazu auffordern, Sicherheitsfunktionen auf deinem Gerät oder in deinem Account zu deaktivieren.

So erkennst du betrügerische E-Mails und Nachrichten

Betrüger versuchen, die E-Mail- und Textnachrichten von echten Unternehmen zu kopieren, um dich dazu zu verleiten, dass du persönliche Daten und Passwörter herausgibst. Anhand der folgenden Merkmale kannst du einen möglichen Phishing-Betrugsversuch per E-Mail erkennen:

Die E-Mail-Adresse oder Telefonnummer des Versenders passt nicht zu dem Unternehmen, zu dem er angeblich gehört.

Die zur Kontaktaufnahme mit dir verwendete E-Mail-Adresse oder Telefonnummer weicht von der E-Mail-Adresse oder Telefonnummer ab, die du bei dem entsprechenden Unternehmen hinterlegt hast.

Ein Link in einer Nachricht sieht vertrauenswürdig aus, doch die URL stimmt nicht mit der Website des Unternehmens überein.[2]

Die Nachricht unterscheidet sich in ihrem Aussehen erheblich von anderen Nachrichten, die du von dem Unternehmen erhalten hast.

Du wirst in der Nachricht nach persönlichen Daten wie der Kreditkartennummer oder dem Passwort für einen Account gefragt.

Die Nachricht trifft unaufgefordert ein und enthält einen Anhang.

Du erhältst verdächtige Telefonanrufe oder Voicemails

Betrüger rufen oft von gefälschten Telefonnummern an, die die Telefonnummern von Unternehmen wie Apple kopieren, und behaupten häufig, dass dein Account oder Gerät verdächtige Aktivitäten aufweist, um deine Aufmerksamkeit zu erregen. Oder sie verwenden Schmeicheleien oder Drohungen, um dich dazu zu drängen, ihnen Informationen, Geld oder sogar Apple Gift Cards zu geben.

Wenn du einen unerwünschten oder verdächtigen Anruf von jemandem erhältst, der behauptet, von Apple oder vom Apple Support zu stammen, lege einfach auf.

Du kannst betrügerische Anrufe bei der Federal Trade Commission (nur USA) unter reportfraud.ftc.gov melden oder dich an deine örtliche Strafverfolgungsbehörde wenden.

Du bemerkst verdächtige Kalenderereignisse

Wenn du eine unerwünschte oder verdächtige Kalendereinladung in Mail oder Kalender erhältst, kannst du es in iCloud als Junk melden. Wenn du ungewollt einen Spam-Kalender abonniert hast, kannst du ihn löschen.

Dein Webbrowser zeigt störende Popups an

Wenn dir beim Surfen im Internet ein Popup oder eine Meldung über einen kostenlosen Gewinn, Sicherheitsprobleme oder Viren auf deinem Gerät angezeigt wird, schenke dem keinen Glauben. Bei diesen Arten von Popups handelt es sich normalerweise um betrügerische Werbung, die dich dazu verleiten soll, Schadsoftware zu laden oder dem Betrüger persönliche Informationen oder Geld zu geben.

Rufe die Nummer nicht an und folge nicht den Links, um den Preis zu beanspruchen oder das Problem zu beheben. Ignoriere die Nachricht und navigiere einfach von der Seite weg oder schließe das gesamte Fenster bzw. den Tab.

Du wirst zum Download von Software aufgefordert

Sei äußerst vorsichtig, wenn du Inhalte aus dem Internet herunterlädst. Einige im Internet gefundene Downloads enthalten möglicherweise nicht die behauptete Software oder enthalten Software, die du nicht erwartest oder wünschst. Dies schließt Apps ein, die Konfigurationsprofile installieren möchten, welche dann dein Gerät steuern können. Nach einer Installation kann solche unbekannte oder unerwünschte Software übergriffig und ärgerlich werden und sogar deinen Mac beschädigen und deine Daten stehlen.

Um unerwünschte, gefälschte oder schädliche Software zu vermeiden, installiere Software aus dem App Store, oder beziehe sie direkt von der Entwickler-Website. Hier erfährst du, wie du Software auf deinem Mac sicher öffnest oder unerwünschte Konfigurationsprofile von deinem iPhone, iPad oder iPod touch entfernst.

[2] Um das Ziel eines Links auf deinem Mac zu überprüfen, bewege den Mauszeiger über den Link, um die URL zu sehen. Wenn du die URL in der Statusleiste von Safari nicht sehen kannst, wähle „Darstellung“ > „Statusleiste einblenden“. Auf einem iOS-Gerät kannst du deinen Finger auf den Link legen.