techsoup GLOBAL

Sichere Internet-nutzung für Non-Profits - 12 Tipps

Diese Anleitung für die sicherere Nutzung des Internets ist für gemeinnützige Organisationen bestimmt.

Als gemeinnützige Organisation sind Sie auf das Wohlwollen und das Vertrauen Ihrer Unterstützer angewiesen. Daher ist es von größter Bedeutung, dass Sie Ihre Daten und Ihre Infrastruktur schützen. Diese Anleitung dient dazu, Sie dabei zu unterstützen.

Unsere 12 Tipps umfassen vier Hauptbereiche:

Im Büro

Es gibt einige grundsätzliche Dinge, die Sie und Ihre Mitarbeiter bei der Arbeit im Büro bedenken sollten. Lernen Sie diese kennen, bevor es zu spät ist.

Soziale Medien

Soziale Medien sind die am häufigsten besuchten Webseiten online. Seien Sie sich der Do's and Don'ts bewusst, wenn Sie diese nutzen, sowohl privat als auch beruflich.

Außerhalb des Büros

Die meisten Mitarbeiter verwenden mehrere Geräte (wie Laptops, Mobiltelefone und Tablets) und nutzen diese auch in öffentlichen Bereichen. Beachten Sie diese hilfreichen Tipps, wenn Sie außerhalb Ihres Büros tätig sind.

Die Cloud

Online-Anwendungen speichern Ihre Daten im Internet. Diese Tipps helfen Ihnen, dass die Daten sicher und zuverlässig geschützt bleiben.

techsoup GLOBAL

1 Machen Sie Hackern das Leben schwer

Seien Sie klug im Umgang mit Passwörtern. Neben der physischen Sicherheit Ihres Büros, sind Passwörter der nächste, wichtigste Punkt, den es zu beachten gilt. Nutzen Sie starke Passwörter, mit einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen. Dies hilft Ihnen, sich gegen Hacker zu verteidigen, die auf Basis zufälliger und systematischer Vermutungen versuchen, Passwörter zu knacken, die auf häufig verwendeten Wörtern basieren. Daher sollten Sie zusätzlich folgendes beachten:

- ◯ Nutzen Sie verschiedene Passwörter für verschiedene Webseiten. Verwenden Sie Passwort-Management-Software, um sich daran zu erinnern.
- ◯ Um Passwortwiederherstellungen vorzubeugen, die auf gemeinhin bekannten Informationen beruhen (Ihr Geburtsdatum, Ihr erstes Auto oder der Name Ihres Haustieres), überlegen Sie, ob Sie damit zusammenhängende aber völlig unsinnige Antworten nutzen könnten. Zum Beispiel könnten Sie stattdessen die Stadt nehmen, in der eines Ihrer Kinder geboren wurde, das Auto Ihres Nachbarn oder die Farbe Ihres Haustiers.

Aktualisieren Sie Ihre Software. Hacker nutzen Schwachpunkte, die in häufig verwendeter Software festgestellt werden, wie in Betriebssystemen, Office-Software und Internetbrowsern. Um das zu vermeiden sollten Sie:

- ◯ Alle Updates in Ihren Softwareprogrammen installieren und, wenn möglich, automatische Updates aktivieren.
- ◯ Anti-Malware-Software auf allen Computern installieren. Wenn Sie mehrere vernetzte Computer nutzen, verwenden Sie Software, die Sicherheit auf Unternehmensebene bietet und auch alle Updates zentral verwaltet.

Blockieren Sie Spam. Es ist von großer Bedeutung, einen guten Spamschutz zu haben. Spam ist der am häufigsten genutzte Weg, Computer mit Viren zu infizieren, oder so genanntes „Social Engineering" durchzuführen. („Social Engineering" bedeutet, dass Kriminelle Menschen psychologisch so manipulieren, dass diese vertrauliche Informationen teilen.)

2 Betrug vermeiden

Verhindern Sie Social Engineering. Selbst wenn Sie starke Passwörter haben, können Sie so ausgetrickst werden, dass Sie die Daten über Social Engineering zur Verfügung stellen. Um derartigen Betrug zu verhindern, denken Sie daran:

- ◯ In der Regel werden Sie nie per E-Mail oder Telefon nach Zugangsdaten oder persönlichen Daten gefragt. Geben Sie also diese Daten nicht preis, wenn Sie eine solche E-Mail doch einmal erhalten; selbst dann nicht, wenn der Absender legitim erscheint.
- ◯ Suchen Sie nach einem Beweis, dass eine solche E-Mail oder Webseite betrügerische Absichten hat. Seien Sie misstrauisch, wenn Sie falsch geschriebene Wörter, Links zu nicht existierenden, oder nicht passenden Webseiten oder zu Angeboten finden, die zu gut sind, um wahr zu sein.

Achten Sie auf Ransomware. Eine Art von Malware, genannt Ransomware, wurde entwickelt, um ahnungslose Nutzer zu betrügen. Diese spielt Ihnen vor, dass Ihr Gerät mit einem Computervirus infiziert ist und dass Sie gebührenpflichtig eine Software herunterladen müssen, die Ihren Computer reinigt. Verlassen Sie sich auf renommierte Sicherheitssoftware, wie die, die Sie bei Stifter-helfen.net erhalten.

Surfen Sie sicher im Internet. Prüfen Sie, dass eine Webseite als sichere Quelle und als legitim gilt, bevor Sie Kontoinformationen oder sonstige persönliche Daten eingeben. Eine sichere Webseite hat eine URL, die mit **https://**. beginnt. Zusätzlich hat die Adressleiste auf einer sicheren Webseite möglicherweise einen grünen Hintergrund (dies hängt von dem Browser ab, den Sie verwenden). Prüfen Sie, ob Ihre Organisation ein Computer- oder Nutzerprofil hat, mit dem die finanziellen Transaktionen Ihrer Organisation durchgeführt werden (wie Lohnabrechnungen oder Spenden). Ein dafür bestimmter Computer oder ein entsprechendes Nutzerprofil sollte lediglich minimalen Internetzugang und keinen Zugriff auf E-Mails haben.

3 Stellen Sie Richtlinien für Mitarbeiter und Freiwillige auf

Alle Mitarbeiter und Freiwillige sollten diese Anleitung lesen. Zusätzlich dazu sollten sie über die aktuellsten Sicherheitsrisiken aufgeklärt werden. Darüber hinaus wird folgendes empfohlen:

- ◯ Erstellen Sie eine Passwortrichtlinie für Ihre Organisation und stellen Sie sicher, dass Ihre Mitarbeiter die Passwörter nicht einsehbar und geheim aufbewahren.
- ◯ Wenn ein neuer Mitarbeiter oder Freiwilliger eingestellt wird, schulen Sie diesen so, dass jeder die Risiken kennt und die relevanten Taktiken verinnerlicht, um diese Risiken zu reduzieren.
- ◯ Richten Sie eine Nutzungsrichtlinie für Computer und Mobilgeräte ein und bitten Sie Ihre Mitarbeiter um Bestätigung, dass diese gelesen und verstanden wurde. Diese Richtlinie sollte erklären, was Benutzer mit den Geräten tun dürfen, was installiert und gespeichert werden darf und was außerhalb der Geschäftszeiten zulässig ist. Die Richtlinie sollte auch den Austausch verlorener oder gestohlener Geräte erläutern.
- ◯ Überlegen Sie, ob Sie ein getrenntes Netzwerk einrichten und pflegen können, wie ein Subnetz oder eine drahtloses "Gästenetzwerk" mit strengen Kontrollen. Sollte dies nicht machbar sein, raten wir dazu, dass Mitarbeiter oder Gäste im Allgemeinen nicht die eigenen Geräte im Netzwerk Ihrer Organisation nutzen sollten. Wenn Sie die Nutzung Ihres Netzwerks zulassen, richten Sie auch hier eine entsprechende Nutzungs-Richtlinie ein.

techsoup GLOBAL

4 Sichere Mobilgeräte und externe Arbeitsplätze

Laptops, Tablets und Telefone gehen leicht verloren oder werden gestohlen. Daher:

- ◯ Sollte ein mobiles Gerät niemals der einzige Ort sein, an dem wichtige Datensätze gespeichert sind.
- ◯ Wie bei am Arbeitsplatz verwendeten Computern sollten Sie den Zugriff auf Ihr Gerät mittels PIN, Passwort oder Biometrie schützen.
- ◯ Sollte jedes Gerät, das verloren oder verlegt werden kann, verschlüsselt sein. Diese Vorsichtsmaßnahmen gelten auch für Laptops.
- ◯ Achten Sie auf Malware, wie bösartige Apps, die entwickelt wurden, um Informationen zu stehlen. Überlegen Sie zweimal, bevor Sie eine App installieren, und wenn, installieren Sie sie nur aus bekannten App-Stores.
- ◯ Verwenden Sie GPS und Standortfunktionen auf Ihrem Telefon oder Tablet nur, wenn Sie diese unbedingt benötigen. Es ist richtig, dass diese Funktion für die Personalisierung sehr bequem sein kann. Allerdings sind dadurch Standortdaten in Ihren Status-Posts oder in Bildern enthalten, die Hackern zusätzliche Informationen geben könnten, um Social Engineering anzuwenden.

Wenn Ihr Gerät verloren ging oder gestohlen wurde:

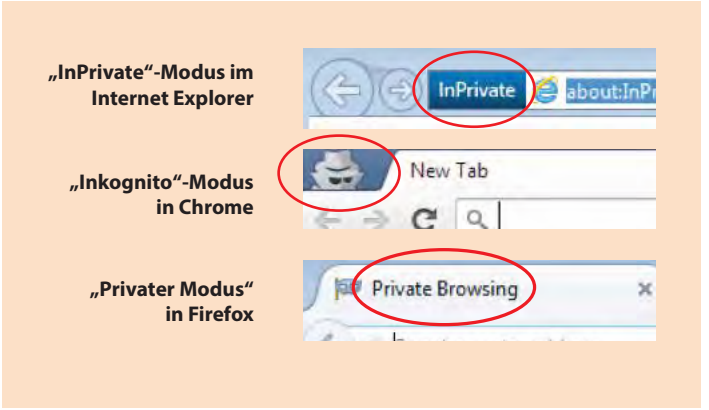
- ◯ Sie können versuchen, das Gerät zu lokalisieren, indem Sie die Telefon-Finder-Funktion nutzen.
- ◯ Wenn Sie das Gerät nicht finden können, können Sie über Remote-Zugriff alle Daten vom Gerät entfernen, wenn es online ist. Alternativ können Sie Einstellungen vornehmen, die per Fernzugriff alle Daten vom verschwundenen Gerät entfernen, sobald es wieder online ist.

5 Seien Sie achtsam, wenn Sie öffentliche Computer verwenden

Sie sollten jeden öffentlichen Computer als Sicherheitsrisiko einstufen. Dies umfasst öffentliche Computer an Flughäfen oder in Geschäften oder in Computerräumen, die für die Öffentlichkeit zugänglich sind. Diese Computer sollten sich bereits im "Kiosk-Modus" befinden, das heißt, die Daten werden nicht gespeichert, gehen Sie aber immer davon aus, dass dies nicht der Fall ist.

Wenn Sie einen öffentlichen Computer verwenden müssen:

- ◯ Verwenden Sie ihn niemals für Finanztransaktionen.
- ◯ Wenn Sie auf E-Mails oder soziale Medien zugreifen, verwenden Sie den "Privatmodus" des Browsers, der keine Informationen speichert, nachdem Sie den Browser schließen. Sie können auf diese Funktion über die Haupt-Toolbar zugreifen, über die Sie üblicherweise eine neue Registerkarte oder ein neues Fenster öffnen.



Achten Sie in öffentlichen Bereichen auch besonders auf die physische Sicherheit:

- ◯ Lassen Sie den Computer nicht unbeaufsichtigt, während sensible Informationen am Bildschirm angezeigt werden.
- ◯ Achten Sie auf Personen, die Ihnen über die Schulter sehen könnten.
- ◯ Schließen Sie Ihre Geräte oder Laufwerke niemals an einen öffentlichen Computer an.

6 Seien Sie achtsam, wenn Sie öffentliche Wi-Fi-Netze verwenden

Sie sollten alle öffentlichen Wi-Fi-Netzwerke als unsicher behandeln. Das heißt Sie sollten:

- ◯ Öffentliche Wi-Fi-Netzwerke nur verwenden, wenn Sie unwesentliche Dinge im Internet suchen.
- ◯ Niemals finanzielle oder persönliche Transaktionen über ein öffentliches Netzwerk ausführen.
- ◯ Überlegen Sie sicherere Alternativen. Vielleicht können Sie mit einer Person telefonieren oder persönlich mit ihr sprechen, wenn er oder sie verfügbar ist.

Wenn Sie sich doch mit einem öffentlichen Wi-Fi-Netzwerk verbinden müssen:

- ◯ Verbinden Sie sich lieber mit einem Netzwerk, das gesichert ist, als mit einem „offenen". Ein solches Netzwerk hat ein „Schloss"- oder „Schild"-Symbol neben dem Netzwerknamen. Sichere Netzwerke erfordern, dass Sie ein Passwort eingeben oder bestimmten Bedingungen zustimmen, bevor Sie fortfahren können.
- ◯ Achten Sie auf ähnlich benannte Netzwerke, die konzipiert sind, um Nutzer zu täuschen, damit Sie sich anmelden. Diese Netzwerke könnten Ihren Traffic abfangen. Wenn Sie Zweifel haben, fragen Sie jemanden vor Ort, um sicherzugehen, welches Netzwerk das richtige ist.

Ein virtuelles privates Netzwerk (VPN) kann einige dieser Risiken senken, wenn Sie öffentliche Netzwerke nutzen. Wenn Sie Mitarbeiter haben, die über eine Remoteverbindung arbeiten oder häufig auf Reisen sind, überlegen Sie, ob Sie ein VPN einrichten können.

techsoup GLOBAL

7 Soziale Medien sind sozial (nicht „privat“)

Es ist wichtig zu verstehen, dass alles, was online ist, sowohl dauerhaft verfügbar als auch übertragbar ist. Alles, was Sie auf Seiten sozialer Medien tun, ist auch für Werbetreibende sichtbar und für die Öffentlichkeit oft zugänglicher, als Sie glauben.

Wenn Sie soziale Medien verwenden, sollten Sie immer:

- ◯ sorgfältig abwägen, wir öffentlich Sie Ihr Profil und Ihre Informationen machen möchten.
- ◯ jede Seite untersuchen und beurteilen - besonders die Einstellungen zum Datenschutz - bevor Sie sie verwenden.
- ◯ einen angemessenen Rahmen definieren, für das, was Sie online teilen.
- ◯ wählerisch sein, wen Sie als „Freunde“ akzeptieren
- ◯ vorsichtig sein, wenn Sie jemanden persönlich treffen, den Sie zuerst online getroffen haben, unabhängig davon ob aus persönlichen oder beruflichen Gründen. Tun Sie dies an einem öffentlichen Ort und lassen Sie andere wissen, wo Sie sich aufhalten.

Soziale Medien sind ein beliebter Ausgangspunkt für Phishing und Social Engineering. (Phishing ist der Versuch, sensible Informationen zu erhalten, wie Benutzernahmen, Passwörter und Kreditkartendaten [und manchmal, indirekt, auch Geld]. Der Phisher gibt sich in elektronischer Kommunikation als vertrauenswürdige Institution oder Person aus) Dies entsteht daraus, dass Nutzer eher dem trauen, was ihre „Freunde“ posten. Seien Sie in solchen Fällen genauso achtsam wie Sie es bei E-Mails und Webseiten wären.

8 Teilen Sie nicht alles

Persönliche Daten können für Betrug, Identitätsdiebstahl oder dafür verwendet werden, Sie ausfindig zu machen. Dinge, die Sie online posten, können außerdem Ihren zukünftigen Arbeitsplatz, Kredite oder Versicherungsanträge beeinflussen und können auf Ihre Organisation negativ zurückfallen.

Um sicherzustellen, dass Ihre Privatsphäre, Sicherheit und Ihr Ruf geschützt sind, wenn Sie soziale Medien nutzen:

- ◯ Posten Sie nur Dinge, von denen Sie möchten, dass Sie der Öffentlichkeit bekannt sind.
- ◯ Posten Sie keine unangemessenen Bilder, Videos oder Kommentare.
- ◯ Wenn Sie einen Standortdienst verwenden, überlegen Sie, ob Sie den Personenkreis einschränken sollten, der auf diese Informationen zugreifen kann. Daten über Ihren Standort können leicht für kriminelle Machenschaften verwendet werden. Kriminelle könnten Sie ausspionieren, Ihnen folgen oder etwas stehlen.

9 Seien Sie vorsichtig, wenn Ihre Organisation soziale Medien nutzt

Besondere Vorsicht muss walten, wenn Mitarbeiteroder Freiwillige soziale Medien im Namen Ihrer Organisation nutzen. Wie für die Sicherheit, gilt für neue Angestellte und Freiwillige, die in sozialen Medien aktiv sind, dass sie auch in den sozialen Medien verstehen, was von ihnen erwartet wird.

- ◯ Mitarbeiter sollten sich darüber bewusst sein, dass sie nur auf eine Art und Weise posten oder antworten sollten, die mit den Werten der Organisation übereinstimmt. Sie sollten für Ihre Organisation Richtlinien für die Nutzung sozialer Medien errichten.
- ◯ Wenn mehrere Nutzer ein gemeinsames Konto verwenden, ist es von Vorteil zu bestimmen, wann dies welcher Mitarbeiter tut.
- ◯ Einige Dienste bieten verschiedene Rollen mit verschiedenen Nutzungsrechten an. Teilen Sie Ihren Mitarbeitern entsprechende Rollen zu.
- ◯ Wenn Sie Ihre Kooperationspartner etc. "markieren" oder in einem Post in sozialen Medien erwähnen, können Sie unbeabsichtigt mehr Informationen offenlegen, als Sie vielleicht möchten, nutzen Sie diese Funktion daher mit Bedacht.
- ◯ Wenn Sie nicht ausdrücklich die Erlaubnis Ihrer Partner erhalten habe, deren Bilder zu verwenden, machen Sie deren Gesichter auf Fotos und in Videos unkenntlich.

Foto (diese Seite): Twin Design / Shutterstock.com

techsoup GLOBAL

10 Seien Sie vorsichtig beim Umgang mit Logins und überlegen Sie, ob Sie den Zugang zu geteilten Dateien beschränken sollten

Wenn Ihre Organisation Cloud-Dienste nutzt, kann sich jeder, der über die Zugangsdaten verfügt, zu diesem Dienst anmelden. Jeder Mitarbeiter oder jeder Freiwillige sollte individuelle Anmeldedaten haben.

Viele Dienste nutzen eine Zwei-Faktoren-Authentifizierung, wobei die Anmeldung mit einem zweiten Gerät, zum Beispiel einem Mobiltelefon, bestätigt werden muss. Aktivieren Sie diese Funktion wenn möglich, besonders für kontobezogene Änderungen, wie Passwörter.

Nutzer müssen stets vorsichtig sein, wem sie Zugang zu Ihren Dokumenten und Dateien gewähren. Dokumente und Dateien online sind so konzipiert, dass sie einfach geteilt werden können. Bestätigen Sie die richtigen E-Mail-Adressen, wenn Sie Zugang gewähren und überlegen Sie, ob die Person sowohl Lese- als auch Schreibrechte für den Inhalt benötigt.

11 Machen Sie sich mit den Richtlinien Ihres Cloud-Anbieters vertraut

Als Nutzer von Cloud-Diensten sollten Sie die Richtlinien Ihres Anbieters in Bezug auf Eigentum der Daten und deren Ablageort kennen.

Wenn Behörden bei Ihrem Cloud-Anbieter nach Ihren Daten verlangen, wird dieser dem wahrscheinlich zustimmen und Ihre Daten an die Behörde übermitteln. Wenn Ihre Organisation einer solchen Datenübermittlung an die Regierung eher kritisch gegenüber steht, ist die Cloud möglicherweise nicht die richtige Wahl für Sie. Cloud-Daten können darüber hinaus auch leichter ins Visier Ihrer Konkurrenten geraten.

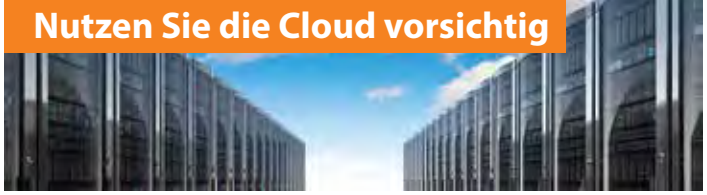
Unter Umständen könnte eine „private" oder eine „hybride" Cloud anstelle einer öffentlichen Cloud eher zu Ihrer Organisation passen. Für welche Option Sie sich entscheiden, hängt davon ab, welchen Grad an Exklusivität Ihre Organisation benötigt.

12 Denken Sie an Offline-Backups

Seien Sie darauf vorbereitet, dass ein Online-Backup-Dienst einmal nicht zur Verfügung stehen könnte. Dies gilt sowohl für kostenlose als auch für zahlungspflichtige Produkte. Bevor Sie Daten in der Cloud ablegen, denken Sie darüber nach, welche Folgen es für den Betrieb in Ihrer Organisation hätte, wenn diese Daten einmal nicht zur Verfügung stünden.

Laden Sie Kopien Ihrer wichtigsten Daten herunter, sodass Sie auf diese zugreifen können, selbst wenn der Cloud-Dienst nicht zur Verfügung steht. Ihre Daten sollten in einem üblichen Format exportiert werden, sodass Sie sie ohne viel Aufwand direkt verwenden können. Wenn dies nicht der Fall ist, überlegen Sie, ob Sie zu einem Anbieter wechseln können, der diese Möglichkeit anbietet.

Es gibt oft ein Protokoll der Änderungen an Online-Dokumenten. Prüfen Sie diese Änderungen regelmäßig auf ungewöhnliches Verhalten.



Die Erstellung und Übersetzung dieses Guides wurde unterstützt von Microsoft.