Spam-Mails, Social Engineering, Phishing – das sind nur einige der Betrugsmethoden, die im Internet angewendet werden. Wie Sie als Verein oder andere gemeinnützige Organisationen das Internet sicher nutzen können, hat „Partner TechSoup“ in einem 3-teiligen Leitfaden zusammengestellt. Teil 1

In insgesamt 12 Tipps erfahren Sie, wie Sie Ihre Infrastruktur und damit auch die Daten Ihrer Mitglieder, Spender und Förderer schützen können. Den Auftakt machen Tipp 1 bis 4.

Ein Artikel von TechSoup USA

UNSERE 12 TIPPS UMFASSEN VIER HAUPTBEREICHE

In Ihrem Büro

Es gibt einige grundlegende Dinge, an die Sie und Ihre Mitarbeiter denken sollten, wenn Sie im Büro arbeiten. Lernen Sie sie, bevor es zu spät ist.

Social Media sicher nutzen

Social Media Seiten sind die Seiten, die online am häufigsten besucht werden. Achten Sie auf einige Dos und Don’ts, wenn Sie sie benutzen, sowohl im privaten als auch im beruflichen Umfeld.

Außerhalb Ihres Büros

Die meisten Mitarbeiter verwenden mehrere Geräte (z.B. Laptops, Mobiltelefone und Tablets) und verwenden sie in öffentlichen Bereichen. Beachten Sie diese nützlichen Tipps, wenn Sie nicht in Ihrem Büro sind.

Die Cloud sicher nutzen

Online-Anwendungen speichern Ihre Daten im Internet. Diese Tipps helfen Ihnen, sicherzustellen, dass Ihre Daten sicher und unversehrt bleiben.

1 MACHEN SIE ES HACKERN SCHWER

Optimale Passwörter. Nach der physischen IT-Sicherheit Ihres Büros sind Passwörter der nächste wichtige Schritt. Verwenden Sie sichere Passwörter mit einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen. Dies wird Ihnen helfen, sich gegen Hacker zu verteidigen, die zufällige und systematische Schätzungen vornehmen, die auf häufig verwendeten Wörtern basieren.

Verwenden Sie unterschiedliche Passwörter für verschiedene Websites. Verwenden Sie eine Passwortverwaltungssoftware, damit Sie sich an die Passwörter erinnern können.

Um die unbefugte Passwort-Wiederherstellung zu verhindern, die auf allgemein bekannten Informationen basiert (Ihr Geburtsdatum, das Modell Ihres Autos oder der Name Ihres

Haustieres), überlegen Sie, ob Sie verwandte, aber unsinnige Antworten verwenden können. Sie können beispielsweise die Stadt, in der ein Kind geboren wurde, das Modell des Autos Ihres Nachbarn oder die Farbe Ihres Haustieres verwenden.
Verwenden Sie nach Möglichkeit eine Zwei-Faktor-Authentifizierung. Die Zwei-Faktor-Authentifizierung erfordert, dass Sie neben der Eingabe eines Passworts auch einen Code eingeben, der Ihnen entweder über eine Textnachricht, eine Codegenerator-App oder ein Hardware-Token zur Verfügung gestellt wird.
Aktualisieren Sie Ihre Software. Hacker nutzen Schwachstellen, die in häufig verwendeter Software wie Ihrem Betriebssystem, der Bürosoftware und Webbrowsern zu finden sind. Um dies zu verhindern:
Installieren Sie alle Updates für Ihre Softwareprogramme und stellen Sie sie so ein, dass sie automatisch aktualisiert werden, wenn dies möglich ist.
Installieren Sie Anti-Malware-Software auf allen Computern. Wenn Sie über mehrere vernetzte Computer verfügen, verwenden Sie Software, die Sicherheit auf Unternehmensebene bietet und Updates verwaltet.
Blockieren Sie Spam-Mails. Es ist wichtig, einen guten Spam-Blocker zu haben. Spam ist der häufigste Weg, auf dem Sie mit einem Computervirus infiziert werden oder über Social Engineering manipuliert werden können. (Bei Social Engineering handelt es sich um eine Technik, mit der Cyberkriminelle versuchen, Menschen psychologisch zu manipulieren, damit sie vertrauliche Informationen preisgeben.)

2 TÄUSCHUNG VERHINDERN

Vermeiden Sie Social Engineering. Selbst wenn Sie über starke Passwörter verfügen, können Sie dazu gebracht werden, Informationen über Social Engineering bereitzustellen. Um diese Betrügereien zu vermeiden, denken Sie an Folgendes:
Sie werden niemals aufgefordert, Zugangsdaten oder persönliche Daten in einer E-Mail oder am Telefon anzugeben. Geben Sie diese Informationen nicht an, auch wenn der Absender legitim erscheint.
Suchen Sie nach Beweisen, die darauf hindeuten, dass eine E-Mail oder Website betrügerisch ist. Seien Sie misstrauisch, wenn Sie falsch geschriebene Wörter, Links zu einer unabhängigen Website oder Angebote sehen, die zu gut sind, um wahr zu sein.
Hüten Sie sich vor Ransomware. Ransomware ist eine bösartige Schadsoftware, die entwickelt wurde, um arglose Benutzer zu betrügen. Sie überzeugt Sie, dass Ihr Gerät mit

einem Computervirus infiziert ist und dass Sie eine Gebühr zahlen müssen, um Software herunterzuladen, die Ihren Computer desinfiziert. Verlassen Sie sich auf seriöse Sicherheitssoftwareprogramme, wie sie beispielsweise von Stifter-helfen angeboten werden.
Surfen Sie sicherer im Internet. Überprüfen Sie, ob eine Webseite legitim ist, bevor Sie Bankinformationen oder persönliche Daten eingeben. Geben Sie beispielsweise die Adresse der Website Ihrer Bank manuell in die Adressleiste Ihres Browsers ein, anstatt in einer E-Mail auf einen Link zu klicken, und stellen Sie sicher, dass es keine Tippfehler gibt.
Suchen Sie außerdem nach Websites, deren Adressen mit „https“ beginnen. Dies bedeutet, dass die Website eine Verschlüsselung verwendet, um die Daten zu schützen, die zwischen Ihnen und dieser Website übertragen werden. Die meisten großen Websites verwenden HTTPS-Verschlüsselung.
Überlegen Sie auch, ob Sie einen Computer oder Benutzerprofil haben sollten, das für die finanziellen Transaktionen Ihrer Organisation reserviert ist (wie Gehaltsabrechnungen oder Spenden). Ein dedizierter Computer oder Benutzerprofil hätte idealerweise nur minimalen Internetzugang und keinen Zugang zu E-Mails.

3 LEGEN SIE RICHTLINIEN FÜR HAUPT- UND EHRENAMTLICHE MITARBEITER FEST

Alle Mitarbeiter und Freiwilligen sollten diesen Leitfaden lesen. Darüber hinaus sollten sie über kürzlich entdeckte Sicherheitsrisiken informiert werden. Außerdem:
Richten Sie eine Passwortrichtlinie für Ihre Organisation ein und stellen Sie sicher, dass die Mitarbeiter die Passwörter außer Sichtweite haben und geheimhalten.
Wenn neue Mitarbeiter oder Freiwillige an Bord kommen, schulen Sie sie so, dass jeder sowohl die Risiken als auch Maßnahmen zur Minimierung dieser Risiken versteht. Legen Sie eine Nutzungsrichtlinie für Computer und mobile Geräte fest und lassen Sie Ihre Mitarbeiter bestätigen, dass sie diese gelesen und verstanden haben. Ihre Richtlinie sollte erklären, was Benutzer mit den Geräten machen dürfen, was installiert und gespeichert werden darf und was außerhalb der Geschäftszeiten erlaubt ist. Die Richtlinie sollte das Vorgehen bei Verlust oder Diebstahl eines Geräts definieren.
Überlegen Sie, ob Sie ein Teilnetzwerk wie ein Subnetz oder ein drahtloses „Gast“-Netzwerk mit strengen Kontrollen einrichten und unterstützen können. Wenn dies nicht möglich ist, raten wir in der Regel davon ab, dass Mitarbeiter oder Gäste ihre eigenen Geräte im Netzwerk Ihres Unternehmens verwenden. Wenn Sie es Personen gestatten, sich in Ihr Netzwerk einzubinden, implementieren Sie eine Richtlinie, die für Ihr Unternehmen geeignet

ist.

Legen Sie Mindestnormen für die Nutzung persönlicher Geräte für Arbeitszwecke fest. So können Sie beispielsweise verlangen, dass Mitarbeiter eine Antivirensoftware installiert haben und Sicherheitspatches installieren, sobald sie verfügbar sind. Sie sollten den Mitarbeitern auch raten, keine persönlichen Konten für Cloud-Speicher, E-Mails oder andere Dienste zu verwenden, die sensible Daten aus der direkten Kontrolle Ihres Unternehmens herausnehmen.

Verwenden Sie nach Möglichkeit „Single Sign-On“. Diese Technologie ermöglicht Ihnen, die Kontosicherheit im gesamten Unternehmen einfacher zu verwalten, indem Sie die Anzahl der Konten für verschiedene Dienste reduzieren. Außerdem ist es einfacher, den Zugriff auf kritische Systeme bei Bedarf zu widerrufen.

4 SICHERE MOBILE GERÄTE UND REMOTE-WORKSTATIONS

Laptops, Tablets und Telefone können leicht verloren gehen oder gestohlen werden. Deshalb,

Ein mobiles Gerät sollte niemals der einzige Speicherort für wichtige Daten sein.

Wie bei den Bürocomputern, schränken Sie den gelegentlichen Zugriff auf Ihr Gerät mit einer PIN oder einem Passwort ein.

Jedes Gerät, das verloren gehen oder verlegt werden kann, sollte verschlüsselt werden. Diese Vorsichtsmaßnahme sollte auch Laptops umfassen.

Achten Sie auf Malware, wie z.B. bösartige Anwendungen, die sind, Informationen zu stehlen. Überlegen Sie es sich zweimal, bevor Sie eine App installieren, und tun Sie dies nur in seriösen App-Stores.

Verwenden Sie ein Kabelschloss, um Ihren Laptop zu sichern, wenn er unbeaufsichtigt bleibt, oder verstauen Sie ihn an einem sicheren Ort wie einem verschlossenen Schrank.

Verwenden Sie GPS- und Ortungsfunktionen auf Ihrem Handy oder Tablet nur dann, wenn Sie es benötigen. Obwohl diese Funktion sehr komfortabel für die Personalisierung sein kann,können Standortdaten, die in Ihren Statusposts oder Bildern enthalten sind, Hackern jedoch zusätzliche Informationen geben, die sie für das Social Engineering nutzen können.

Wenn Ihr Gerät verloren geht oder gestohlen wird.

Sie können Ihr Gerät vielleicht finden, wenn Sie die Funktion „Find my iPhone“ oder „Find my Device“ des jeweiligen Gerätes verwenden.

Wenn Sie es nicht finden, können Sie möglicherweise alle Daten aus der Ferne vom Gerät

löschen, wenn es online ist. Oder Sie können alle Daten beim nächsten Online-Start des Geräts aus der Ferne löschen.
Urheber: TechSoup October 2018

Quelle: www.hausdesstiftens.org

Related Post

Unsicherheiten der Wolken

Sozial ist nicht privat

Sicherheit im Netz