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 „TechSoup“ in einem 3-teiligen Leitfaden zusammengestellt. Teil 2

Im zweiten Teil des Leitfadens „Mehr Sicherheit im Internet“ erfahren Sie, was Sie beachten sollten, wenn Sie öffentliche Computer oder öffentliche WLAN-Netzwerke nutzen müssen. Außerdem gibt es Tipps zum Umgang mit sozialen Medien.

Ein Artikel von TechSoup USA

5 SEIEN SIE VORSICHTIG, WENN SIE ÖFFENTLICHE COMPUTER VERWENDEN.

Sie sollten jeden öffentlichen Computer als Sicherheitsrisiko betrachten. Dazu gehören öffentliche Computer an Flughäfen oder Geschäften oder Computerlabore, die öffentlichen Zugang bieten. Diese Computer sollten sich bereits in einem „Kiosk-Modus“ befinden, in dem die Daten nicht gespeichert werden, aber gehen Sie nie davon aus, dass dies der Fall ist.

Wenn Sie einen öffentlichen Computer verwenden müssen:

Verwenden Sie diesen niemals für finanzielle Transaktionen.

Wenn Sie auf E-Mails oder soziale Medien zugreifen, verwenden Sie den „privaten“ Modus des Browsers, der keine Informationen speichert, nachdem Sie den Browser geschlossen haben. Sie können darauf über die Hauptsymbolleiste zugreifen, wo Sie normalerweise eine neue Registerkarte oder ein neues Fenster öffnen.

Melden Sie sich von allen Benutzerkonten ab und schließen Sie alle offenen Browserfenster, wenn Sie fertig sind.

In einem öffentlichen Raum müssen Sie sich auch besonders der physischen Sicherheit bewusst sein.

Lassen Sie den Computer nicht unbeaufsichtigt mit vertraulichen Informationen auf dem Bildschirm.

Achten Sie auf Personen, die Ihnen über die Schulter schauen könnten. Vermeiden Sie es, an sensiblen Projekten in einer überfüllten Umgebung wie z.B. in einem Bus zu arbeiten.

Schließen Sie Ihre Geräte oder Laufwerke niemals an einen öffentlichen Computer an.

6 SEIEN SIE VORSICHTIG, WENN SIE ÖFFENTLICHES WI-FI VERWENDEN.

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

Verwenden Sie öffentliche Wi-Fi-Netzwerke nur für belangloses Surfen im Internet.

Führen Sie niemals finanzielle oder persönliche Transaktionen über ein öffentliches Netzwerk

durch.
Überlegen Sie sich sicherere Alternativen. Überprüfen Sie, ob Sie mit einer Person per Telefon oder persönlich sprechen können, wenn sie verfügbar ist.
Wenn Sie sich mit einem öffentlichen WLAN-Netzwerk verbinden müssen.
Verbinden Sie sich mit einem Netzwerk, das eine gewisse Sicherheit garantiert, und nicht mit einem „offenen“. Ein solches Netzwerk hat ein „Schloss“- oder „Schutzschild“ -Symbol, das sich neben dem Netzwerknamen befindet. Für sicherere Netzwerke müssen Sie ein Passwort eingeben oder einigen Bedingungen zustimmen, bevor Sie fortfahren können.
Hüten Sie sich vor ähnlich benannten Netzwerken, die dazu gedacht sind, Benutzer zu täuschen, damit sie sich einloggen. Diese Netzwerke können auf Ihren Browser-Traffic belauschen. Bitten Sie im Zweifelsfall jemanden an diesem Ort, zu überprüfen, welches Netzwerk das richtige ist.
Besuchen Sie nur Websites, die eine verschlüsselte Verbindung haben (suchen Sie nach Webseitenadressen, die mit „https“ beginnen). Dadurch wird verhindert, dass potenzielle Lauscher Ihr Surfen abhören können.
Ein Virtual Private Network (VPN) kann dazu beitragen, einige dieser Risiken bei der Nutzung öffentlicher Netzwerke zu minimieren. Wenn Sie Mitarbeiter haben, die remote arbeiten oder häufig unterwegs sind, überlegen Sie, ob Sie ein VPN einrichten können.
Wenn Sie Mitarbeiter haben, die häufig an öffentlichen Orten arbeiten, sollten Sie den Kauf von Wi-Fi-Hotspots in Betracht ziehen, die es Ihren Mitarbeitern ermöglichen, sich über ein mobiles Breitbandnetzwerk zu verbinden und das öffentliche Wi-Fi vollständig zu umgehen.

7 SOZIALE MEDIEN SIND SOZIAL (NICHT „PRIVAT“).

Alles, was Sie online veröffentlichen, bleibt dauerhaft bestehen und ist auch übertragbar. Alles, was Sie auf einer Social Media-Website tun, ist auch für Werbetreibende zugänglich und kann öffentlicher zugänglich sein, als Sie es sich vorstellen können.
Wenn Sie soziale Medien nutzen:
Überlegen Sie sorgfältig, wie öffentlich Ihre Profile und Informationen sein sollen.
Untersuchen und bewerten Sie jede Website – insbesondere die Datenschutzeinstellungen -, bevor Sie sie nutzen.
Setzen Sie angemessene Grenzen für das, was Sie online teilen.
Seien Sie selektiv gegenüber Personen, die Sie als „Freunde“ akzeptieren.
Seien Sie wachsam, wenn Sie jemanden persönlich treffen, den Sie zum ersten Mal online

getroffen haben, unabhängig davon, ob es sich um persönliche oder berufliche Gründe handelt. Das Treffen sollte nur an einem öffentlichen Ort stattfinden und Sie sollten andere über Ihren Aufenthaltsort informieren.
Social Media ist auch ein beliebter Einstieg für Phishing und Social Engineering. (Phishing ist der Versuch, sensible Informationen wie Benutzernamen, Passwörter und Kreditkartendaten (und manchmal auch indirekt Geld) zu erhalten. Der Phisher gibt sich als vertrauenswürdige Einheit oder Person in einer elektronischen Kommunikation aus.) Dies liegt daran, dass Benutzer von Natur aus eher darauf vertrauen, was ihre „Freunde“ posten. Seien Sie genauso wachsam wie bei E-Mails und Websites.

8 GRENZEN SIE EIN, WIE VIEL SIE TEILEN.

Personenbezogene Daten können verwendet werden, um Sie zu betrügen, Ihnen nachzustellen oder Sie zu finden. Dinge, die Sie online veröffentlichen, können sich auch auf Ihre zukünftige Bewerbung um einen Job, einen Kredit oder eine Versicherung auswirken und negativ auf Ihre Organisation ausstrahlen.
Um sicherzustellen, dass Sie Ihre Privatsphäre, Sicherheit und Ihren Ruf schützen, wenn Sie Social Media nutzen, sollten Sie:
Nur Dinge veröffentlichen, die Sie auch gerne mit einer größeren Öffentlichkeit teilen wollen.
Veröffentlichen Sie keine unangemessenen Bilder, Videos oder Kommentare.
Wenn Sie einen Standortservice nutzen, überlegen Sie, ob Sie einschränken sollten, wer auf diese Informationen zugreifen darf. Angaben zu Ihrem Standort können leicht für kriminelle Zwecke verwendet werden. Kriminelle könnten Sie ausspionieren, Ihnen folgen oder etwas stehlen.

Quelle: www.hausdesstiftens.org