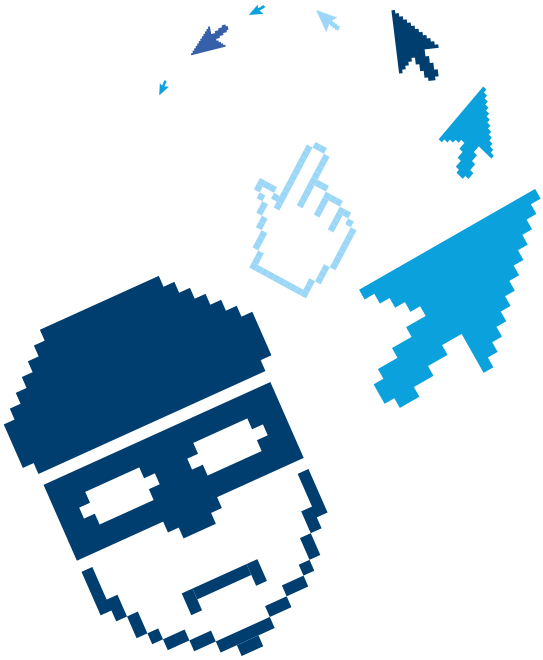
3 Regeln für soziale Netzwerke, die Sie noch heute umsetzen sollten

Persönliche Gedanken, Urlaubsfotos, Treffen mit Bekannten, Freunden oder Kollegen: So ziemlich alles wird heute in den sozialen Netzwerken geteilt. Tabus gibt es kaum. Völlig unabhängig davon, ob Sie es gut finden, dass Privates zunehmend öffentlich gemacht wird, bleibt es eine Tatsache, dass Sie (und Ihre Familie und Freunde) von dieser Verschiebung auf die eine oder andere Weise betroffen sind.

proofpoint.

Natürlich hat die Vernetzung über das Internet viele Vorteile. Gleichzeitig lauern auf diesen ausgesprochen öffentlichen Plattformen auch viele Gefahren. Wer diese minimieren will, sollte folgende drei Regeln beherzigen (und andere ebenfalls dazu anhalten):



Tipp 1: Überprüfen Sie regelmäßig die Privatsphäre-Einstellungen

Falls Sie die Datenschutz- und Privatsphäre-Einstellungen der sozialen Netzwerke, in denen Sie aktiv sind, noch nie überprüft haben, wird es allerhöchste Zeit! (Und wenn Sie jüngere Kinder haben, die in sozialen Netzwerken unterwegs sind, überprüfen Sie deren Einstellungen am besten gleich mit.) Bei Plattformen wie Twitter und LinkedIn ist das Konzept eher darauf ausgerichtet, dass eingestellte Inhalte für die Allgemeinheit zu sehen sind. Andere (wie Facebook, Snapchat und Instagram) leben vom Austausch zwischen einzelnen Personen. Sie sollten daher verstehen, wie Datenschutz in den einzelnen sozialen Netzwerken funktioniert, und die Kontoeinstellungen entsprechend vornehmen.

Grundsätzlich gilt:

- Gehen Sie nicht davon aus, dass die Standardeinstellungen ausreichen. Viele Anwendungen sehen standardmäßig wenig Privatsphäre und Datenschutz vor, damit Profile und Beiträge leicht gefunden werden und Reaktionen erzeugen können.
- Gerade deshalb werden soziale Netzwerke systematisch nach persönlichen und geschäftlichen Informationen durchforstet, die sogenanntes Social Engineering oder sogar Cyberkriminalität ermöglichen. Wenn Sie also Daten öffentlich machen, sollten Sie sich stets bewusst sein, dass Betrüger diese Angaben gegen Sie einsetzen können, indem sie damit beispielsweise gefälschten E-Mails, Telefonanrufen oder sonstigen Versuchen der Kontaktaufnahme einen seriösen Anstrich geben.
- Denken Sie außerdem daran, dass sich die Datenschutzrichtlinien und entsprechenden Einstellungen im Laufe der Zeit immer wieder ändern können. Es ist daher ratsam, die Einstellungen regelmäßig zu überprüfen. Das gilt insbesondere nach Updates von Apps der sozialen Netzwerke.

proofpoint.

GELÖSCHTE BEITRÄGE SIND NICHT UNBEDINGT ENTFERNT. „PRIVATE“ NACHRICHTEN BLEIBEN NICHT ZWINGEND PRIVAT. BEITRÄGE ETWA AUF SNAPCHAT, DIE ANGEBLICH NACH EIN PAAR SEKUNDEN „AUTOMATISCH GELÖSCHT“ WERDEN, SIND DAMIT KEINESFALLS UNWIDERRUFLICH FORT.

Tipp 2: Gehen Sie davon aus, dass alle Aktivitäten und Daten in öffentlichen Netzwerken öffentlich sind

Dies mag auf den ersten Blick wie ein Widerspruch zu Tipp 1 wirken, aber soziale Netzwerke sind eben ein zweischneidiges Schwert, da Datenschutz- und Privatsphäre-Einstellungen nur bis zu einem bestimmten Punkt schützen. Sobald Sie etwas mit jemandem teilen, entzieht es sich Ihrem Einfluss.

Beiträge in sozialen Netzwerken sind letztlich wie Textnachrichten: Sobald Sie eine Nachricht verschicken, können die Empfänger sie problemlos an andere weiterleiten. Sie können auch einen Screenshot der Nachricht erstellen und diesen im sozialen Netzwerk posten. Und jeder, der die Nachricht dort sieht, kann sie an seine Kontakte weitergeben. Was sich hier vielleicht hypothetisch anhört, kommt tatsächlich öfter vor als gedacht. Selbst wenn eine Nachricht eigentlich als rein privater Austausch zwischen Ihnen und dem Empfänger gedacht ist: Einmal abgeschickt, existiert so etwas wie Datenschutz oder Privatsphäre nicht mehr.

Das gilt auch für soziale Netzwerke. Gelöschte Beiträge sind nicht unbedingt entfernt. „Private“ Nachrichten bleiben nicht zwingend privat. Beiträge etwa auf Snapchat, die angeblich nach ein paar Sekunden „automatisch gelöscht“ werden, sind damit keinesfalls unwiderruflich fort.

Beispiele hierfür sind inzwischen laufend in den Medien zu finden, wenn etwa gelöschte „kontroverse“ Tweets in Form von Screenshots weiterleben. Für das Treiben in den sozialen Netzwerken interessieren sich längst nicht mehr nur Betrüger. Zunehmend machen auch Personalabteilungen und Arbeitgeber Entscheidungen von den Informationen abhängig, die sie dort finden – und zwar sowohl mit Blick auf künftige Beschäftigungsverhältnisse als auch auf bestehende. Daher sollten Sie immer davon ausgehen, dass alles, was Sie posten, trotz aller festgelegten Einschränkungen zum Schutz Ihrer Daten und Privatsphäre im Zweifelsfall öffentlich zugänglich ist.

Tipp 3: Stellen Sie Fragen

Wir können gar nicht oft genug darauf hinweisen: Betrüger und Cyberkriminelle lieben soziale Netzwerke. Konten in sozialen Netzwerken sind wahre Fundgruben für persönliche Informationen. Zudem kann sich in diesen Netzwerken problemlos jeder als eine andere Person ausgeben. Die von Betrügern und Fälschern ausgehenden Gefahren sind sehr real. Es drohen finanzielle Schäden, Rufschädigung und manchmal sogar Gefahren für die persönliche Sicherheit.

Bevor Sie also auf einen Link klicken, eine Kontaktanfrage akzeptieren oder eine Datei herunterladen, bedenken Sie die möglichen Folgen, falls die dahinterstehende Person nichts Gutes im Schilde führt. Folgendes sollten Sie sich immer fragen:

Kenne ich die betreffende Person persönlich bzw. vertraue ich dieser Verbindungsmethode?

Die sicherste Faustregel für soziale Netzwerke (und ein grundsätzlich guter Rat für Minderjährige) lautet: Keine Kontaktanfragen von Personen annehmen, die man nicht schon mal persönlich getroffen hat. Das ist zwar (insbesondere auf Twitter) nicht immer möglich, aber es ist immer sinnvoll, darüber nachzudenken, welche Informationen für Ihre Kontakte sichtbar sind. Die meisten Datenschutz- und Privatsphäre-Einstellungen zielen auf eventuelle Spione außerhalb Ihrer Kontakte ab. Damit greifen sie nicht mehr, sobald Sie einer Person Zugang gewährt haben.

3 Regeln für soziale Netzwerke, die Sie noch heute umsetzen sollten

IM INTERNET WIMMELT ES VON SCHÄDLICHEN LINKS UND ANZEIGEN. BESONDERS OFT FINDET SICH BEIDES IN SOZIALEN NETZWERKEN. GEKÜRZTE URLS SIND BESONDERS GEFÄHRLICH, WEIL MAN DEREN ZIEL NICHT SEHEN KANN.

Gehört diese Person bereits zu meinen Kontakten?

Die Konten in sozialen Netzwerken sind oft das Ziel von Betrügern, die sich als andere Personen ausgeben. Sicher haben Sie schon von Vorfällen mit geknackten (mittels kompromittiertem Kennwort) oder duplizierten Konten von Freunden oder Bekannten gehört. Vielleicht haben Sie das sogar selbst schon erlebt. Falls Sie also bei einer Kontaktanfrage einen Verdacht in dieser Richtung haben, fragen Sie bei Ihren Freunden oder Bekannten nach oder melden Sie die verdächtige Aktivität, bevor Sie die Kontaktanfrage annehmen.

Wirkt es seriös?

Soziale Netzwerke stecken voller sogenannter „Clickbaits“. Gelockt wird mit angeblichen kostenlosen Gutscheinen, Zugang zu Premium-Inhalten, Anreißern für Sensationsgeschichten, Tratsch über Promis und grundsätzlich allem, was Leute dazu bringt, etwas anzuklicken. Betrüger erstellen gefälschte Profile und Geschäftsseiten (auch als „Pretexting“ bezeichnet). Dabei verwenden sie häufig bekannte Markennamen, unglaubliche Angebote und dramatische Schlagzeilen. Halten Sie sich von diesen Fallen fern, die einfach zu gut klingen. (Und verbreiten Sie diese Links auch in keinem Fall weiter!)

Misstrauisch werden sollten Sie zudem grundsätzlich auch, wenn Freunde oder Bekannte plötzlich seltsame Inhalte posten (z. B. mehrfach Werbung für hochpreisige Sonnenbrillen) oder unvermittelt um Geld oder Informationen bitten. Konten in sozialen Netzwerken werden regelmäßig geknackt. Anschließend jagen die Hacker oft ganz schnell Beiträge und Nachrichten raus, um einen Erfolg zu erzielen, bevor der Betrug auffliegt. Falls Sie den Verdacht haben, dass ein Konto gehackt wurde, benachrichtigen Sie die Betroffenen nach Möglichkeit über einen vertrauenswürdigen Kanal (Textnachricht, Telefon, E-Mail) oder melden Sie das Konto.

Weiß ich mit Sicherheit, dass dieser Link/diese Datei sicher ist?

Im Internet wimmelt es von schädlichen Links und Anzeigen. Besonders oft findet sich beides in sozialen Netzwerken. Gekürzte URLs sind besonders gefährlich, weil man deren Ziel nicht sehen kann. Von seriösen Unternehmen werden diese Kurz-Links eingesetzt, wenn Längenbeschränkungen für Beiträge eingehalten werden müssen oder das Display die vollständige URL nicht darstellen könnte. Betrüger verschleiern damit hingegen das wahre Ziel eines Links.

Fazit: Erst Bestätigung einholen, dann klicken. Ob gekürzt oder nicht – scheinbar harmlose Links können Sie ganz schön in die Bredouille bringen. Falls Ihnen etwas merkwürdig vorkommt, lassen Sie die Finger davon. Sie sollten mit sozialen Netzwerken genauso vorsichtig umgehen wie mit E-Mails.

Wie vermittle ich meinen Kindern, wachsam zu sein?

Wenn Sie Kinder haben, sollten Sie grundsätzlich darauf achten, was diese im Internet machen und wer zu ihren Kontakten zählt. Mindestens genauso gut ist es allerdings, in Bezug auf Sicherheit in sozialen Netzwerken proaktiv zu sein. Vermitteln Sie Ihren Kindern, wie sie bewährte Methoden selbst anwenden können. Ermutigen Sie sie, Fragen zu stellen und zu Ihnen zu kommen, wenn sie sich wegen etwas nicht sicher sind.

Die meisten Menschen sind von Natur aus vertrauensvoll und offen. Deshalb müssen wir lernen, welche Informationen wir in sozialen Netzwerken weitergeben können und wo Zurückhaltung angebracht ist. Sicherheit im Internet ist keine statische Angelegenheit. Doch mit diesen Tipps für soziale Netzwerke können Sie den Schutz Ihrer personenbezogenen Informationen bereits erheblich verbessern – obwohl es sich um relativ grundlegende Vorsichtsmaßnahmen handelt.