Sicherheit im Internet

Tracking

Unternehmen, Webseitbetreiber und Kriminelle können mithilfe von Cookies, IP-Adressen ihre Aktivitäten im Netz verfolgen und überwachen.

Cookies erlauben Webseiten ihre Aktivitäten zu verfolgen, um zum Beispiel Nutzerverhalten zu verfolgen. (klick auf Werbebanner oder Videos).
Daten können für Kriminelle Aktivitäten genutzt werden.
(Telefon, Name, andere pers. Daten.)

Gegenmaßnahmen:

- Nicht achtlos zustimmen (auch Datenschutzeinblendungen ab und zu prüfen).
- Sich bei sozialen Netzwerken, Online-Banking-Diensten u. ä. immer wieder mal abmelden.
- Bei Firefox Software wie AdBlock oder Ghostery nutzen.
- Nicht jede Kontaktanfrage in sozialen Netzwerken annehmen
- Sicherheitseinstellung der Sozialen Netzwerke und Google prüfen und einstellen.

Spam (Offiziell Verboten), nur mit ausdrücklicher Erlaubnis erlaubt, die entzogen werden kann.

Massenhafte müllen E-Mails ihr Postfach zu
Schädliche Software kann verbreitet werden
Daten können gestohlen werden

Nicht nur per E-Mail sondern auch über soziale Medien, SMS und Messenger-Dienste um über Ihre Adresse ungewollte Nachrichten zu schicken. Meist unseriöse Finanzprodukte, Dating-Angebote und medizinische Artikel wie Abnehm-Pille.

Manchmal auch täuschend echte Emails von Banken oder z. B. Telekomm oder Inkasso-Unternehmen.

Gegenmaßnahme:

- Regelmäßig Postfach kontrollieren und unerwünschte Mails als „Spam“ kennzeichnen. Meist lernt das Programm selbst mit der Zeit.
- Keine verdächtigen Mails von Unbekannten öffnen.
- Keine Anhänge von unbekannten öffnen.
- 2te Email-Adresse die sie r für Seiten verwenden wenn sie nicht hundertprozentig sicher sind. (Browser-Games, Online-Foren, Gewinnspiele.
- Spam-Filter
- Abmelden, wenn möglich/Die Erlaubnis entziehen
- Betriebssystem und Browser auf dem neuestem Stand halten, Sicherheitsupdates installieren.

Datenlecks – kommt vor wenn Unternehmen gehackt werden

Die „erbeuteten“ Daten können im Internet veröffentlicht werden um Angriff auf ihre Accounts zu nehmen, Identitätsdiebstahl zu begehen, oder Spam-Mails oder andere Betrugs Mails zu versenden.

Persönliche Daten und Passwörter könnten veröffentlicht werden. Ihre Daten sind so leicht für Kriminelle abrufbar und nutzbar
Doxing/ Cybermobbing

Ähnlich wie beim Datenleck können persönliche Daten oder Bilder im Internet veröffentlich werden und zu Cybermobbing verwendet werden

Gegenmaßnahmen

- Passwort regelmäßig ändern
- Software aktuell halten

Identitätsdiebstahl

Betrüger nützen persönliche Daten wie Geburtsdatum, Anschrift, Sozialversicherungsnummer, Kontonummer um diese für kriminelle Zwecke zu missbrauchen.

Plötzlich Rechnungen eines Versandhauses, obwohl sie nicht bestellt haben
Kriminelle könnten mit ihren Daten Online-Shopping betreiben und Straftaten begehen.
Fake- Accounts könnten mit ihren Daten bei Medien oder Online-Versandhäusern erstellt werden.

Gegenmaßnahmen:

- Sichere Passwörter und Software auf dem neuesten Stand
- Vorsicht bei Nutzung von öffentlichen WLAN
- Unverzüglich zur Polizei gehen und Anzeige erstatten. Informieren sie zusätzlich ihren Bekanntenkreis.
- Zahlungsaufforderungen unverzüglich wiedersprechen.
- Keine Zahlungen auf dubiose Mails hin leisten.

Phisihing

Mit Phising gelangen Kriminelle an sensible Daten wie z. B. Kontonummer.
Das Konto könnte geplündert werden.
In Sonderformen wird das Opfer bewusst ausgesucht und mit betrügerischen Nachrichten die gut recherchiert sind, den Betrugsversuch zu verschleiern.

Z. B. auch:
Gewinnversprechen
Versprechen über Erbschaft usw.

Gegenmaßnahmen:

- Auf Hinweise Achten wie fehlende persönliche Anrede, eine schlechte Rechtschreibung und Grammatik, verdächtige Anhänge Betreff nur in Großbuchstaben oder Sonderzeichen usw. achten

Schadsoftware

Durch spezielle Software (Malware und Ransomware, Trojaner) könnte Sicherheitslücken im Browser oder Betriebssystem ausgenutzt werden um ihren PC zu infizieren.

Schädliche Software kann ihren Rechner infizieren und dort reichlich Schaden anrichten. Das reicht von performance-Problemen (Rechner wird langsamer, Popups blockieren die Sicht, bis hin zum Diebstahl ihrer persönlichen Daten.
Bei Ransomware fordern Kriminelle sogar Lösegeld, damit sie ihren PC wieder nutzen können. Dieser Aufforderung auf keinen Fall nachkommen, zumeist sind die Daten ohnehin verloren.

Gegenmaßnahmen

- Software mit Programm ADWARE entfernen (kostenlos), kann nach Nutzung wieder entfernt/Deinstalliert werden.
- Regelmäßige Sicherheitsupdates
- Passwörter regelmäßig ändern
- Schadsoftware entfernen

Fazit:

- Sehr genau lesen!
- Wenn ein Angebot „zu Gut“ ist, Vorsicht walten lassen.
- Zahlungspflichtige Dienste müssen lt. Gesetz deutlich gekennzeichnet sein.
- Vorsicht bei Gewinnspielen. (Gewinnspiele dürfen nicht an Bedingungen gekoppelt sein)
- Keine Kontonummern oder Bankverbindung über Internet eingeben (Pre-Paid-Card nutzen).
- Keine Mails von Unbekannten öffnen.
- Mails von Banken, Inkasso-Unternehmen oder Internetanbietern mit Vorsicht behandeln.
- Regelmäßig Passwörter ändern
- Software aktuell halten
- Bei Verdacht kostenloses Programm wie Adware nutzen.
- Programme nur von seriösen Quellen laden.
- Unbekannten Zahlungsaufforderungen nicht nachkommen, gegebenenfalls Einspruch einlegen oder gleich zu Anwalt oder Polizei gehen.