Datenschutz im Open-Source

In der Open-Source-Welt trägt jeder Einzelne zur globalen Sicherheit bei. Deine Rolle als Mitwirkender beeinflusst Millionen von Nutzern. Erkenne die Wichtigkeit grundlegender Sicherheitsmaßnahmen für die Stabilität und Vertrauenswürdigkeit der Open-Source-Welt.

Dein Sicherheitsleck betrifft uns alle

Vergiss nie: **Deine Sicherheitslücken wirken sich direkt auf andere Projekte aus**. Nutze den Austausch mit Kollegen, um Schwachstellen zu erkennen und zu schließen.

Denke wie ein Hacker!

Der Verlust eines Passworts kann zum Datenleck werden, wodurch sensible Patienteninformationen, wie Rezeptbestellungen oder Rückfragen, gefährdet sind.

Passwort-Verlust vermeiden

- **Copy & Paste**: Sei vorsichtig beim Kopieren und Einfügen von Passwörtern. Ein versehentlicher Klick kann fatale Folgen haben.
- **Passwortschutz**: Gib niemals Passwörter per E-Mail oder Nachricht weiter. Lösche immer alle Nachrichten, die sensible Informationen enthalten könnten. Sei dir der dauerhaften Existenz von Backups bewusst!

Sofortmaßnahmen bei Sicherheitsfehlern

Hoffnung ist keine Strategie: Bedenke, dass Hacker stets nach Schwachstellen suchen und diese innerhalb Sekunden automatisiert ausnutzen. Handel sofort: Wenn ein Fehler passiert ist, handle unmittelbar und beseitige ihn. Zögere nicht, Kollegen um Hilfe zu bitten. Erinnerung: **Das Internet vergisst nie - auch scheinbar gelöschte Daten können weiterhin vorhanden sein.**

Vorkehrungen für den Datenschutz

- **Passwort-Manager:** Nutze einen Passwort-Manager zur sicheren Verwaltung deiner Zugangsdaten.
- **Zwei-Faktor-Authentifizierung:** Schütze deine Konten zusätzlich mit der Zwei-Faktor-Authentifizierung.
- **Starke Passwörter:** Wähle komplexe Passwörter aus einer Mischung von Buchstaben, Zahlen und Sonderzeichen. Mindestens 12 Zeichen sind empfehlenswert.
- **Regelmäßiger Wechsel:** Ändere deine Passwörter regelmäßig und verwende niemals dasselbe Passwort für mehrere Konten.

Vertraue deinem Bauchgefühl

Wenn dein Computer plötzlich ungewöhnlich agiert, könnte es ein Zeichen für eine Infektion sein. Zögere nicht, um Hilfe zu bitten!

E-Mails mit Skepsis begegnen

Bestätige sicherheitsrelevante Vorfälle stets persönlich. Zweifle an E-Mails, wenn sie unerwartet oder seltsam wirken. Statt auf Links zu klicken, kontaktiere den Absender über einen bekannten und sicheren Weg.

E-Mails sind potenzielle Sicherheitsrisiken

Stelle dir vor, ein Hacker hätte Zugriff auf dein Postfach. Lösche E-Mails, die nicht mehr benötigt werden und sei vorsichtig mit den Informationen, die du teilst und speicherst.