

# Die 10 wichtigsten Einstellungen für sicheres Surfen mit dem Internet Explorer.

## 1. Deaktivieren Sie XPS-Dokumente

Die XML Paper Specification (XPS) ist ein Dateiformat für Dokumente, das Microsoft mit Vista eingeführt hat. Angreifer haben einen Heidenspaß, Bild- beziehungsweise Dokumentenformate und Parser für ihre Zwecke zu missbrauchen. Daher gilt laut Forristal: Je weniger Formate der Browser unterstützt, desto besser.

**Und so geht's:** Extras -> Internetoptionen -> Sicherheit -> Internetzone -> Benutzerdefiniert: Stufe anpassen -> XPS-Dokumente: deaktivieren.

**Nachteile:** Diese Einstellung kann das Betrachten von XPS-Dokumenten beeinträchtigen. Microsoft bietet jedoch einen Stand-alone-XPS-Viewer an, der nicht auf den IE angewiesen ist.

## 2. Deaktivieren Sie den Schriftart-Download

Viele Web-Seiten bieten an, sich über den Browser ein Font-File installieren zu lassen, um internationale Schriftzeichen auf der Site korrekt darstellen zu können. Allerdings handelt es sich dabei um ein weiteres Dateiformat – und einen weiteren Angriffsvektor, da Ersteres noch unentdeckte Schwachstellen beherbergen könnte. Wer in der Regel keine fremdsprachigen Websites besuche, benötige das nicht wirklich, so Forristal.

**Und so geht's:** Extras -> Internetoptionen -> Sicherheit -> Internetzone -> Benutzerdefiniert: Stufe anpassen -> Schriftartdownload: deaktivieren.

**Nachteile:** Manche Web-Seiten sind daraufhin möglicherweise weniger hübsch

## 3. Schließen Sie beim Datei-Upload den lokalen Verzeichnispfad aus

Wann immer Sie eine Datei auf einen Web-Server hochladen (etwa ein Bild in Ihren Blog oder Flickr-Account), kann der Browser entweder nur den Dateinamen oder den vollständigen Dateipfad senden – selbst wenn die Web-Seite nur den Dateinamen benötigt. Da der Dateipfad identifizierende Informationen wie den Login-Namen eines PC enthalten kann, ist das riskant. "Sendet der Browser etwa C:\Dokumente und Einstellungen \jforristal\bilder\blog.gif", gibt er meinen Nutzernamen (jforristal) preis", gibt Zscaler-Experte Forristal zu bedenken.

**Und so geht's:** Extras -> Internetoptionen -> Sicherheit -> Internetzone -> Benutzerdefiniert: Stufe anpassen -> Lokalen Verzeichnispfad beim Hochladen von Dateien mit einbeziehen: deaktivieren.

**Nachteile:** keine.

## 4. Deaktivieren Sie die automatische Eingabeaufforderung

Bei vielen Optionen in der Zone "Sicherheit" ist die automatische Eingabeaufforderung, die fragt, was Sie jeweils tun wollen, bereits voreingestellt. Tendieren Sie grundsätzlich dazu, "ja" anzuklicken, wenn Ihnen ein Popup-Fenster präsentiert wird (übrigens keine gute Angewohnheit!), sollten Sie die Option durchweg deaktivieren.

**Und so geht's:** Extras -> Internetoptionen -> Sicherheit -> Internetzone -> Benutzerdefiniert: Stufe anpassen-> Automatische Eingabeaufforderung für ... Anpassen.

**Nachteile:** keine.

## 5. Geben Sie stets Nutzernamen und Passwort ein

Für Heimanwender oder PC-Nutzer außerhalb eines Unternehmens, das Active Directory verwendet, ist es kein Vorteil, die Auto-Logon-Funktion aktiviert zu haben. Forristal empfiehlt, sich nirgendwo im Internet automatisiert einzuloggen. Zwar begrenzt der IE die automatische Anmeldung üblicherweise auf Sites innerhalb der Intranet-Zone - was aber, wenn ein Angreifer den Browser glauben macht, eine Site befinde sich in einer anderen Zone? Für eine Funktion, die man nicht brauche, sei es nicht sinnvoll, dieses Risiko einzugehen, so der Experte

**Und so geht's:** Extras -> Internetoptionen -> Sicherheit -> Internetzone -> Anmeldung -> Nach Benutzername und Passwort fragen.

**Nachteile:** keine.

## 6. Deaktivieren Sie SSL-2.0-Unterstützung

Das Verschlüsselungsprotokoll SSL2 (Secure Sockets Layer) gilt schon lange als unsicher, so Forristal. Ihm zufolge führt jede Website, die lediglich SSL2 und nichts Neuere (etwa SSL3 oder TLS) unterstützt, entweder

Schlechtes im Schilde oder ist so alt, dass sie vor Schwachstellen strotzt und damit für Hacker ein gefundenes Fressen ist.

**Und so geht's:** Extras -> Internetoptionen -> Erweitert -> SSL 2.0 verwenden: nicht anklicken.

**Nachteile:** keine.

## 7. Aktivieren Sie TLS-Unterstützung

TLS (Transport Layer Security) ist eine Weiterentwicklung von SSL, die mehr Sicherheitserweiterungen bietet als SSL3. Die Funktion sollte daher aktiviert sein.

**Und so geht's:** Extras -> Internetoptionen -> Erweitert -> TSL 1.0 verwenden: anklicken.

**Nachteile:** keine.

## 8. Deaktivieren Sie die Suche in der Adressleiste

Forristal rät davon ab, Informationen in die Adressleiste einzugeben und als Suchbegriffe direkt an Suchmaschinen zu schicken. Dabei könne es passieren, dass Daten unerwünscht preisgegeben werden, warnt der Sicherheitsspezialist.

**Und so geht's:** Extras -> Internetoptionen -> Erweitert -> Suchen in Adressleiste: Nicht in Adressleiste suchen.

**Nachteile:** keine.

## 9. Deaktivieren Sie unnötige Add-ons

Es gibt jede Menge Tools von Drittanbietern, die sich in Ihren Browser einklinken. Im Prinzip bietet jedes dieser Add-ons eine Möglichkeit für Hacker, Sie anzugreifen. Daher empfiehlt Forristal, möglichst viele abzuschalten

**Und so geht's:** Extras -> Internetoptionen -> Programme -> Add-Ons verwalten.

**Nachteile:** Leider erschließt sich nicht immer unmittelbar, was man besser in Ruhe lässt und was deaktiviert werden sollte. Laut Forristal tun Anwender dennoch gut daran, die Add-on-Liste nach nicht länger benötigten Tools zu durchforsten. Wer beispielsweise Skype nach einer Versuchsperiode von mehreren Monaten nicht mehr nutzt, könne das Skype-Browser-Add-on getrost abschalten.

## 10. Deinstallieren Sie alte Java-Installationen

Aus unerfindlichen Gründen installieren sich neue Java-Versionen manchmal als komplett neue Versionen statt als Upgrades älterer Releases. Das kann problematisch sein, weil ein Angreifer die älteren Versionen nach wie vor für seine Zwecke missbrauchen könnte – und diese möglicherweise Sicherheitslücken aufweisen, die in der Nachfolgeversion bereits behoben sind. Forristal empfiehlt daher, die Liste der installierten Anwendungen zu überprüfen, zu "Java" zu scrollen und – bis auf die an oberster Stelle aufgeführte – alle Versionsnummern zu entfernen. "Bei dieser Gelegenheit lässt sich auch gleich alles andere deinstallieren, was nicht mehr gebraucht wird – und so die Gesamtangriffsfläche verringern", so der Experte.

**Nachteile:** keine.

Bis auf die Deinstallation alter Java-Versionen lassen sich die aufgeführten Einstellungen schnell wieder rückgängig machen. "Man kann also durchaus damit experimentieren und die Settings ausprobieren – sollten Probleme auftreten, einfach zurückgehen, und alles ist wieder wie vorher".

Quelle: Jeff Forristal, Senior Security Engineer