Porches Security: What you need to know about “mixed content” and your personal data

Introduction: Porches Content, Customization

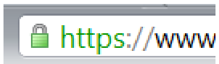
Porches was designed to provide access to “everything UD” you need to study, work and relax at UD. One aspect of this is providing access to important institutional information like class registration, events and financial aid. From the very start we wanted Porches to be a useful homepage as you navigate your online life – providing customization opportunities like adding RSS feeds and website bookmarks.

With the launch of Banner HR/Payroll in January 2011, the institutional information displayed through Porches requires more careful protection than what the site has previously provided. To better protect this data, UD is switching Porches to a secure “https” site effective April 9, 2011. **Please read below to find out what this means to your Porches experience.**

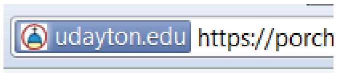
Secure Browsing: http vs. https

Have you ever noticed that some websites begin with “http” while others have an “https”? The difference is security. You can think of the “s” as standing for “secure” – https sites are designed to encrypt data to/from the site so it’s protected as it’s sent across the Internet. Sites that collect credit card payments or display financial data use (or should use!) https.

The lock icon associated with https (see below) is one of the most important cues web sites can provide to users. Without that lock you are left guessing whether your information is being handled securely or not. It’s not an absolute indicator, but certainly a reasonable one.



In addition to a small lock icon, Firefox uses a blue bar in the URL (see below) to indicate site security.



What is “mixed content”?

The content on a web page can come from different places. Some secure https sites allow some linked content (like images) from non-secure http sites. This results in a web page with both secure and non-secure content – “mixed content”. When the browser attempts to load http content on an https page, most browsers will alert you to this by asking if you want to accept the non-secure content. You may have gotten this warning on other websites you’ve visited – it’s a surprisingly common practice, even for some banks and commercial sites.

Your options in Porches

As of April 9, 2011, all default content within Porches is secure and won’t generate any mixed content warnings. However, one of the features of the site is the ability to add content via RSS feeds or embedded websites. When the feed or site includes an image (i.e., ESPN), it’s possible that the image may be transferred using http; if so, your browser will notify you with a warning message.

Option 1: Keep the default, secure Porches layout

If the possibility of falling victim to a scam email or other social engineering threat worries you, your best option is to **leave Porches as-is**. If you don't add RSS feeds or optional, "opt-in" channels, your installation of Porches is perfectly secure.

Option 2: Personalize with external content and be vigilant

If you add personalized content to Porches, be aware that some content may generate mixed content warnings (e.g. RSS feeds with images).

Mixed content doesn't immediately make your secure content visible, but accepting mixed content puts you at greater risk of being targeted with a social engineering scam via suspicious or unknown emails, browser pop-ups, and error messages. **Be extra careful about your computing behavior if you've accepted mixed content**.

F.A.Q.

Why is UD allowing "mixed content" if it poses a security risk?

Security is a balancing act between protecting business/personal interests and allowing users to work/engage. Locking down the site completely would remove the ability for end users to customize Porches – one of the great strengths of the site. Many customizations are completely benign and won't pose any risk. Others, as we've mentioned, may put you at slightly greater risk. Since the potentially sensitive data is personal, not institutional, we've decided the decision on how best to use the site is best left in each user's hands, not ours. That said, Porches is secure in its default configuration – users who don't choose to customize are in a secure environment. Those who do customize just need to be aware of the potential risks involved.

What "sensitive" information is stored in Porches?

Since Banner HR came online in January 2011, Porches has the potential to show you all your HR and Payroll data, salary information, and bank account routing numbers for direct deposit. Supervisors may also have access to "hours worked" for employee time approval queues. Overall, though, the information at risk is personal, not institutional, which is why we're leaving the risk question up to you rather than mandating a campus wide solution.

How risky is accepting mixed content in Porches, really?

We'd suggest "low-risk" because accepting mixed content on a site that uses https increases your risk through targeted "social engineering" exploits – clicking through to a questionable link in an unsolicited email, for example. It doesn't, however, leave you vulnerable to passive attacks such as Firesheep where folks can simply intercept your traffic or hijack your session. Adding mixed content to an https site might make you more of a target, but you have to open the door for the big, bad wolf through unwise computing behavior (reference social engineering warning emails). Our experience with scam emails over the past several years has taught us that about 5% of our campus community falls for social engineering scams.

What happens if I deny mixed content when the error message pops up?
Your Porches session will remain secure if you do not accept mixed content. If you've added RSS feeds or web pages with mixed content, the error message will appear each time you load that content in Porches. If you opt not to allow mixed content, textual elements will still appear but non-secure image elements will not load.

What if I've already customized Porches?
After April 9, some of your customizations (RSS feeds, embedded websites) will begin to generate errors if they contain mixed content.
If you're not comfortable with this, click the "Layout" icon and select "revert to default layout" to return Porches to its initial, secure configuration.

Why are some previously available channels now missing?
On April 9, 2011, we removed all external pre-built channels that included non-secure images. The following channels were pulled from Porches: ESPN, LinkedIn, MSNBC, NY Times, People Magazine, Time.com, and Word of the Day.

Most of these can be re-added securely if you adjust your RSS feed preferences accordingly (see "Can I minimize my risk when adding RSS feeds?" below). ESPN, MSNBC, and NY Times can not be added without generating mixed content warnings. See the RSS reader channel on the "My Tab" tab for instructions on adding RSS feeds.

Can I minimize my risk when adding RSS feeds?
Yes. The "preferences" link within any RSS channel you add gives you the option to choose "no" to "show RSS feed image". In most cases, this will remove mixed content from the feed.

We have found that some RSS feeds – ESPN, MSNBC, and The New York Times, to name a few – will still include linked images (like the "re-tweet" icons) even if you've adjusted this preference. If you're adding new feeds, watch your browser for any warning messages.

Does adding bookmarks put me at risk?
No. Bookmarks simply send you to another website. These don't pose any risk to the secure information you access through Porches.