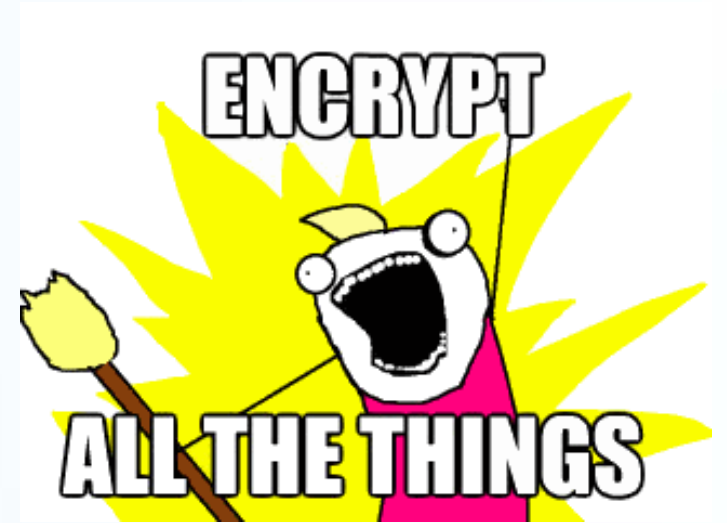


# What you need to know about HTTPS- Part I



UNC Campus Webmasters  
November 16, 2017

Rachell Underhill, Web & Information Services Manager  
The Graduate School

**What is HTTPS?**

# What is HTTPS?

- S = Secure
- Security Certificates confirm a site's identity
- Information is encrypted in transit to prevent snooping or tampering with web pages

# What is HTTPS?

- In the past, websites have deployed HTTPS only when financial transactions take place
- Concerns that HTTPS pages would be slow to load
- SSL Certificates were expensive or complicated to install

# What is HTTPS and why should I care?

- HTTPS is the future and required for HTTP/2 (new version of HTTP)
- No performance penalty
- Certificates are much easier to obtain and install

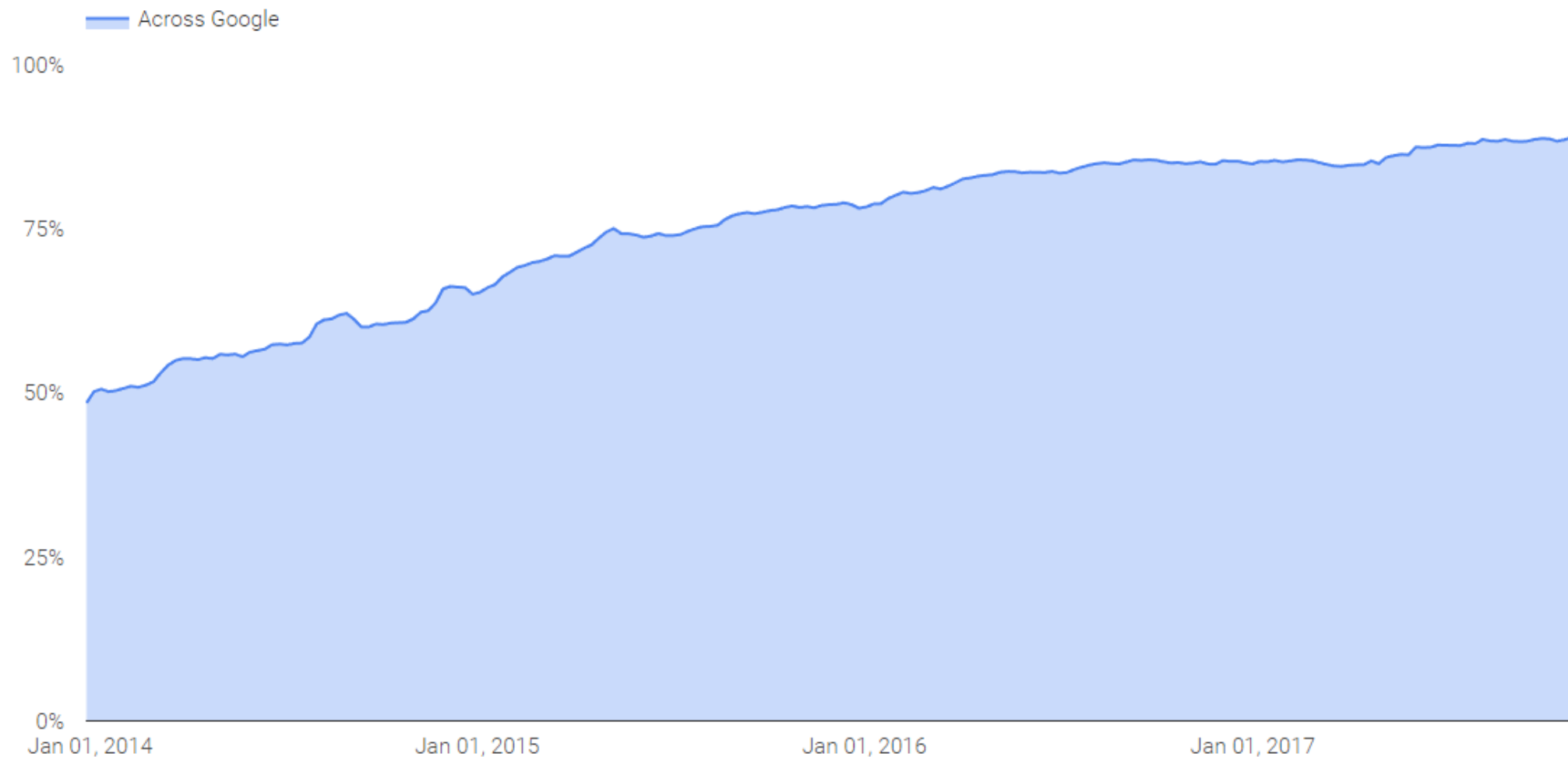
# What is HTTPS and why should I care?

- Google is prioritizing websites that use HTTPS in search results
- Web browsers are notifying users about insecure sites

## Encrypted traffic across Google

Security is a top priority at Google. We are investing and working to make sure that our sites and services provide modern HTTPS by default. Our goal is to achieve 100% encryption across our products and services. The chart below shows how we're doing across Google. For more details on the data, please [visit our FAQ](#).

### WHAT IS ENCRYPTION? [→](#)



**How do web browsers notify users?**



# How do web browsers notify users?

## Warnings include:

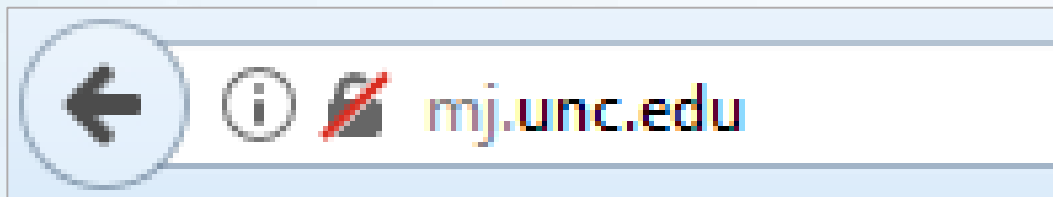
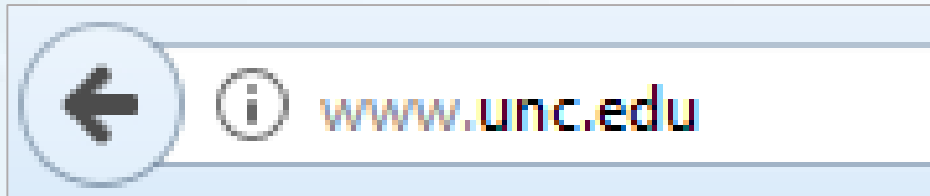
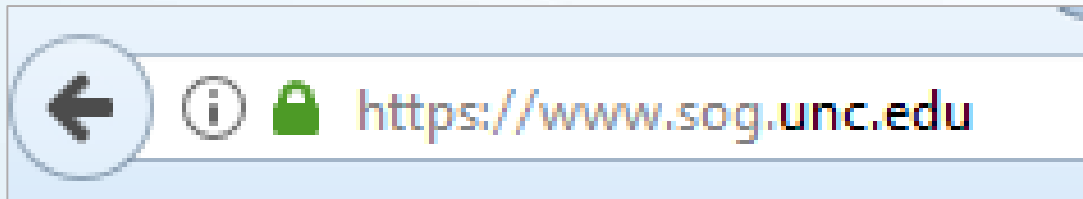
- Mixed content
- Bad certificates
- Forms sent over HTTP
- HTTP sites (coming soon)

# How do web browsers notify users?

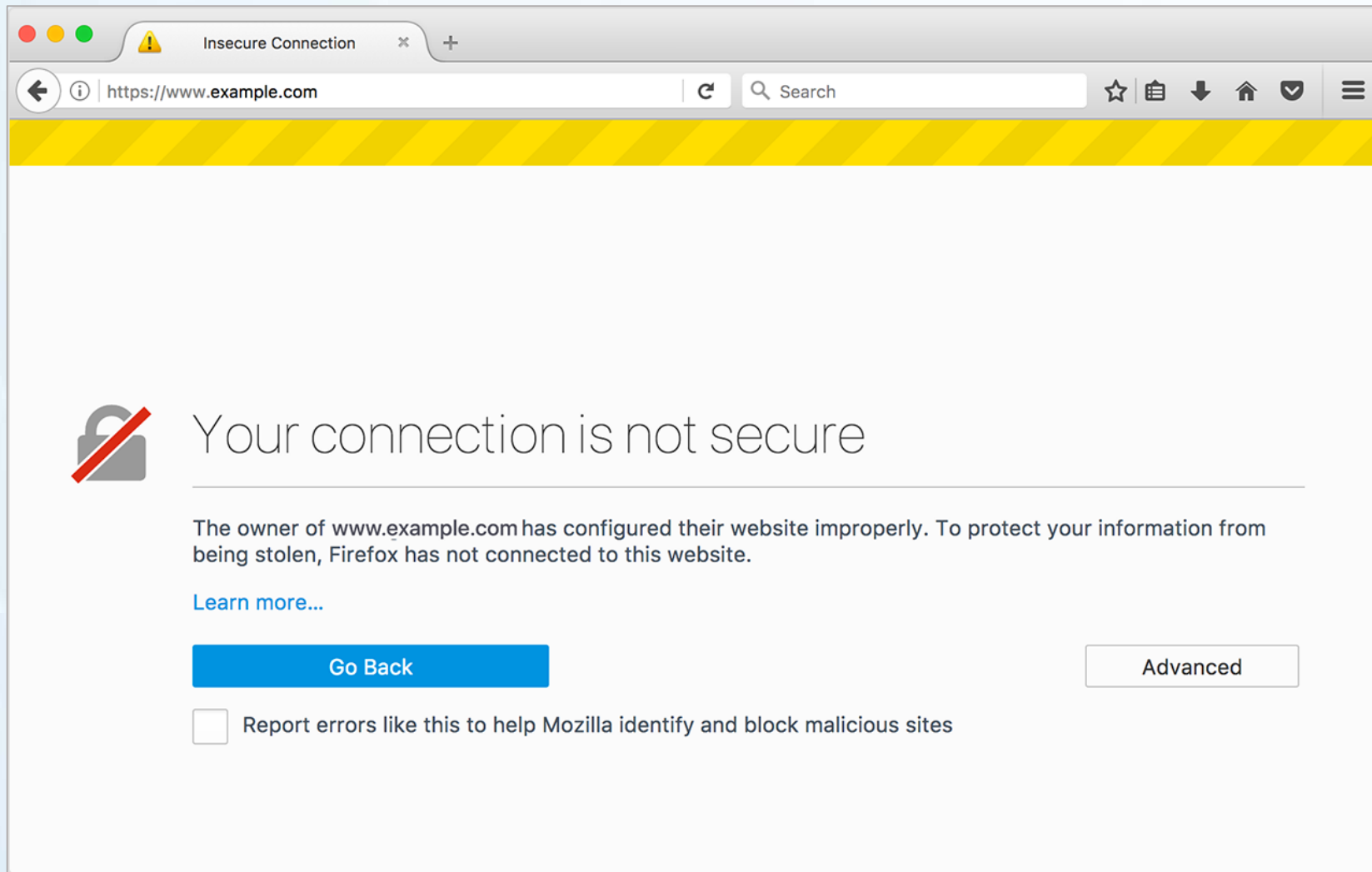


# How do web browsers notify users?

- Firefox Browser




# How do web browsers notify users?



# How do web browsers notify users?

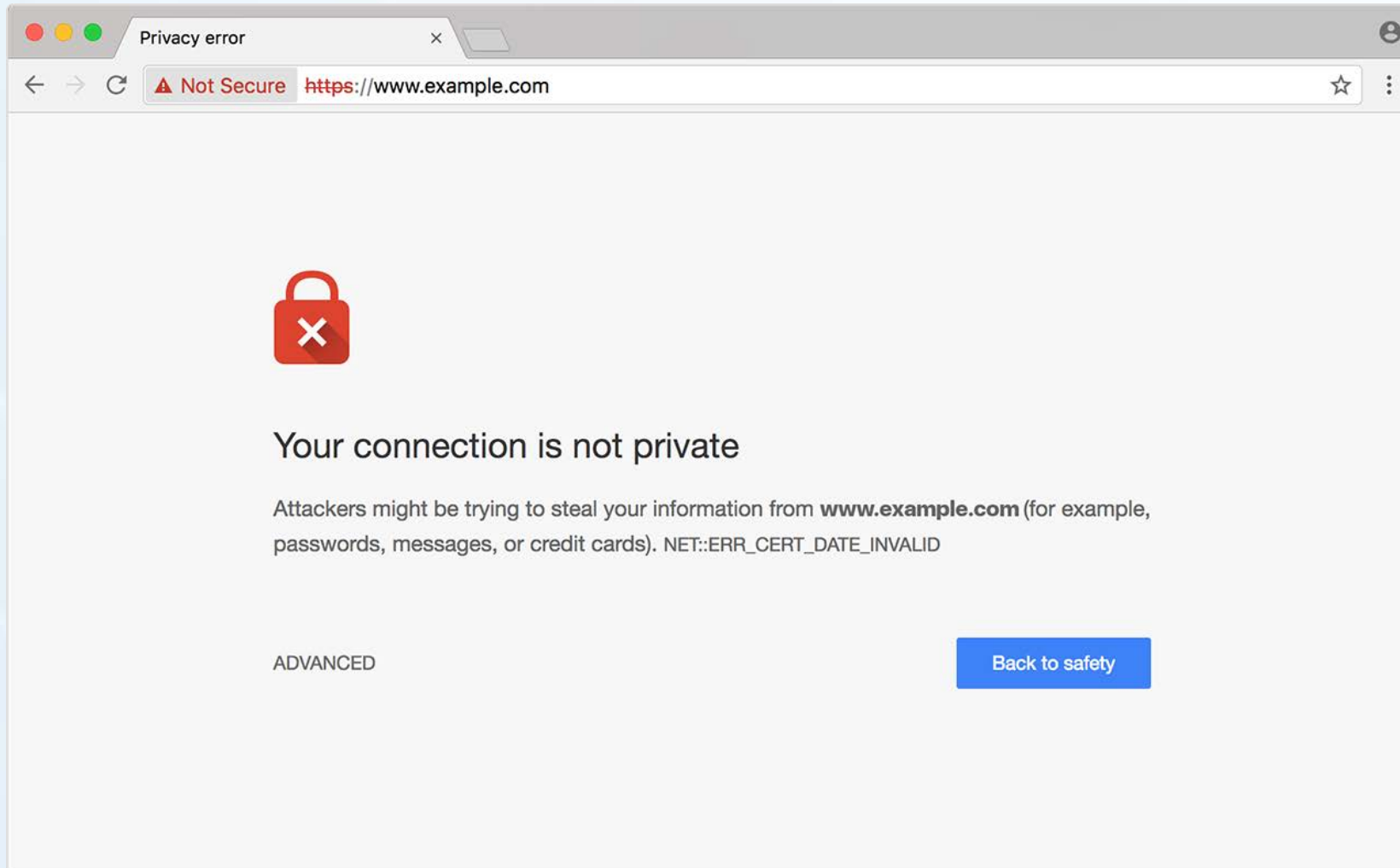
- Chrome Browser

 Secure | <https://www.sog.unc.edu>

 [www.unc.edu](http://www.unc.edu)

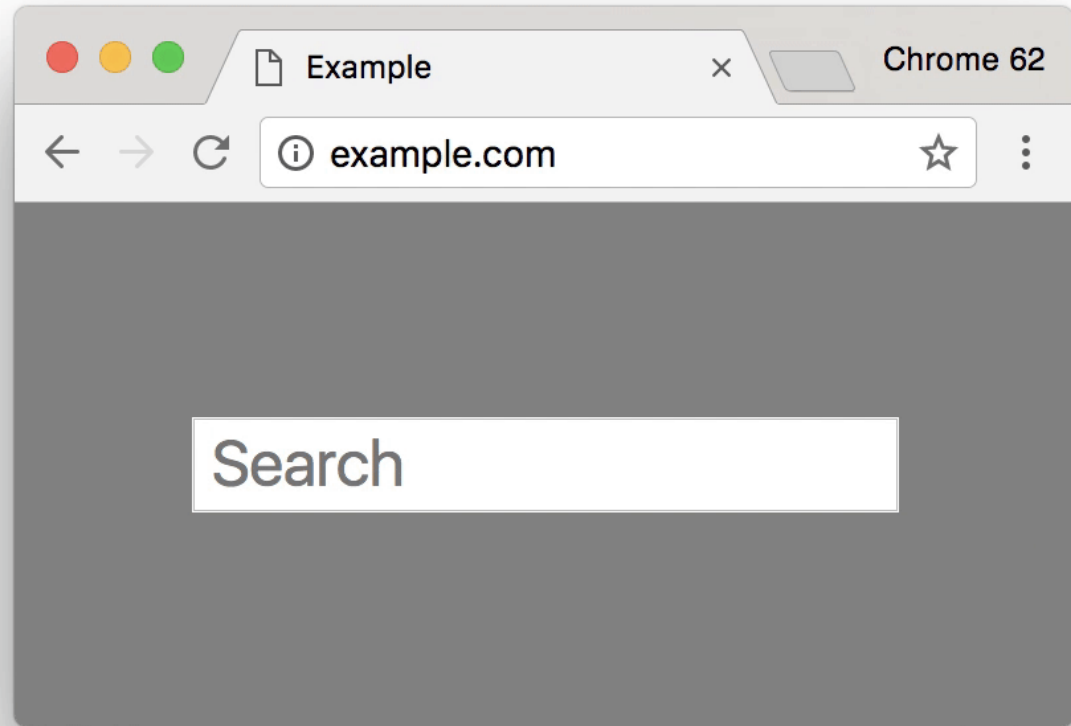
 Not secure | [mj.unc.edu](http://mj.unc.edu)

# How do web browsers notify users?



# How do web browsers notify users?

- Chrome Browser



# How do web browsers notify users?

Eventual treatment of all  
HTTP pages in Chrome:

 **Not secure** | example.com



**What are some common  
pitfalls when switching to  
HTTPS?**

# What are some common pitfalls when switching to HTTPS?

- Invalid or missing SSL certificates
- Mixed Content
- SEO
- Javascript errors, API errors or broken websites

# What are some common pitfalls when switching to HTTPS?

## Mixed Content

- Mixed content occurs when initial HTML is loaded over a secure HTTPS connection, but other resources (such as images, videos, stylesheets, scripts) are loaded over an insecure HTTP connection.

# What are some common pitfalls when switching to HTTPS?

## Mixed Content

- Protocol-relative links no longer recommended

```

```

# What are some common pitfalls when switching to HTTPS?

## Mixed Content

- Find mixed content by visiting your site and viewing error messages in console
- Find and Fix mixed content in your source code

# What are some common pitfalls when switching to HTTPS?

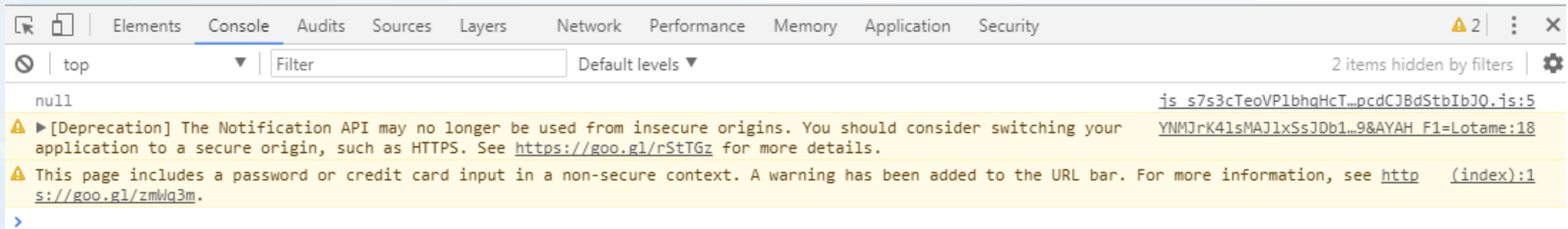
## Find Mixed Content

The screenshot shows a web browser window displaying the UNC School of Media and Journalism website. The address bar shows the URL `mj.unc.edu` and a "Not secure" warning. The website header includes the UNC logo and navigation links. The main content area features a large banner for "SOCIAL MEDIA AND CRISIS COMMUNICATION" with a featured research article by Lucinda Austin. At the bottom, the browser's developer console is open, showing two security warnings:

- A deprecation warning: "[Deprecation] The Notification API may no longer be used from insecure origins. You should consider switching your application to a secure origin, such as HTTPS. See <https://goo.gl/rStTgZ> for more details."
- A mixed content warning: "This page includes a password or credit card input in a non-secure context. A warning has been added to the URL bar. For more information, see <http://goo.gl/zmWg3m>."

# What are some common pitfalls when switching to HTTPS?

## Find Mixed Content



# What are some common pitfalls when switching to HTTPS?

## Find Mixed Content

### View Console:

**Chrome:** CTRL+SHIFT+J (CMD+OPT+J)

**Firefox:** CTRL+SHIFT+K (CMD+OPT+K)

**IE:** F12



# What are some common pitfalls when switching to HTTPS?

## Redirects and SEO

- Use a proper 301 redirect to redirect users from `http://` to `https://`. Do not use a 302 redirect, as this may negatively impact search rankings.

# What are some common pitfalls when switching to HTTPS?

## Redirects and SEO

- Use the canonical link element (`<link rel="canonical">`) to inform search engines that the “canonical” URL for a website uses `https://`.

# What are some common pitfalls when switching to HTTPS?

## JavaScript and/or API errors

- 3<sup>rd</sup> party content
- Forms
- Analytics
- iFrames

# Resources

- [Qualys SSL Labs](#)
- [badssl.com](#)
  
- [Why No Padlock?](#)
- [HTTPS Checker Desktop App](#)
- [Mixed Content Scan](#)

# Thanks!

Presentation notes and extra materials will be posted to **webmasters.unc.edu**.

Rachell Underhill,  
Web & Information Services Manager  
The Graduate School  
[runderhill@unc.edu](mailto:runderhill@unc.edu)  
[@rmunde](https://twitter.com/rmunde)