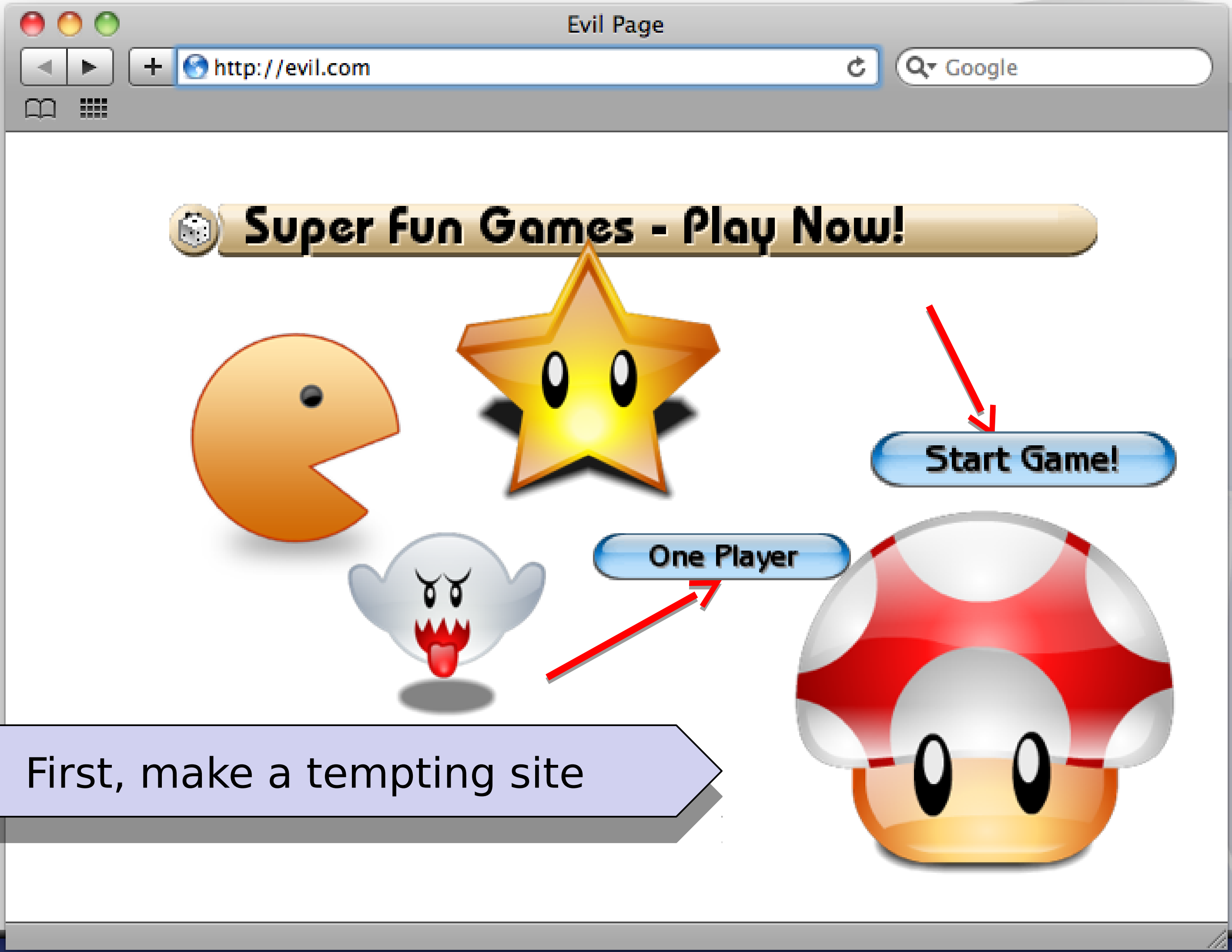
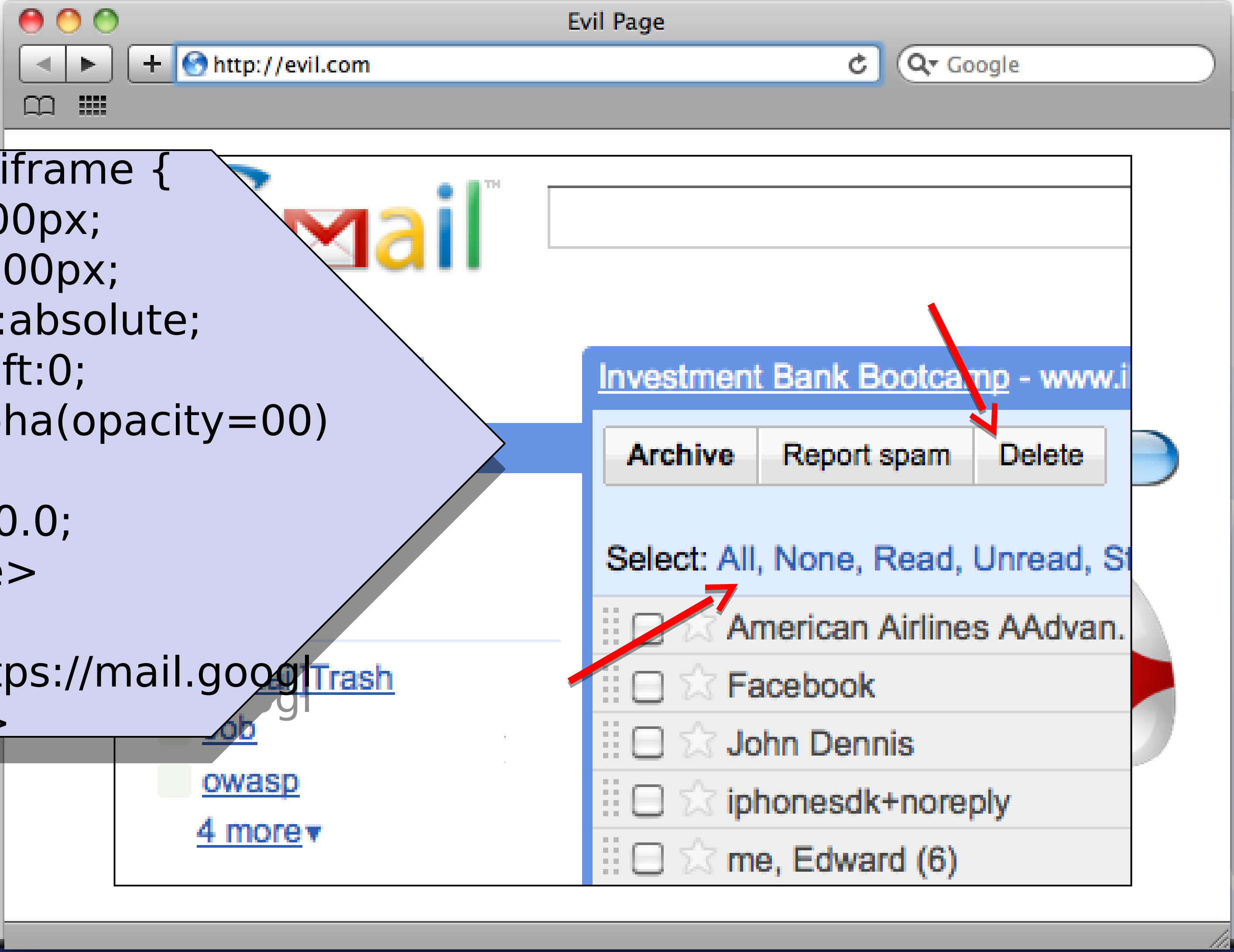
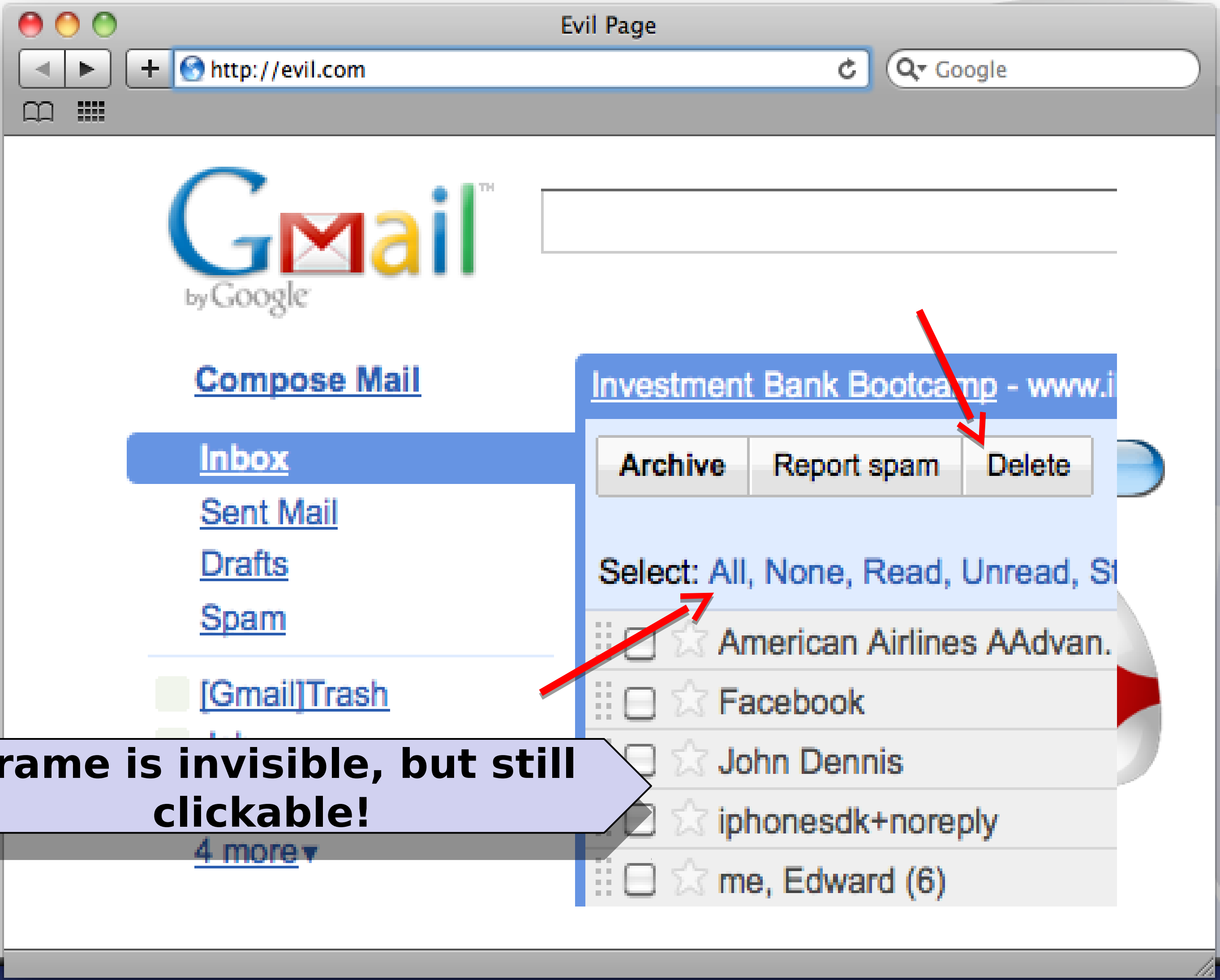
Clickjacking



First, make a tempting site

```
<style>iframe {
width:300px;
height:100px;
position:absolute;
top:0; left:0;
filter:alpha(opacity=00)
;
opacity:0.0;
}</style>
<iframe
src="https://mail.googl
e.com">
```





iframe is invisible, but still clickable!

X-Frame-Options
HTTP Response Header

```
// to prevent all framing of this content
response.addHeader( "X-FRAME-OPTIONS", "DENY" );

// to allow framing of this content only by this site
response.addHeader( "X-FRAME-OPTIONS", "SAMEORIGIN" );

// to allow framing from a specific domain
response.addHeader( "X-FRAME-OPTIONS", "ALLOW-FROM X" );
```

Legacy Browser Clickjacking Defense

```
<style id="antiCJ">body{display:none !
important;}</style>
<script type="text/javascript">
if (self === top)   {
var antiClickjack =
document.getElementByID("antiCJ");
antiClickjack.parentNode.removeChild(antiClickjack)
} else {
top.location = self.location;
}
</script>
```