SECURITY & USER EXPERIENCE

Making the digital world safer one experience at a time

#OReillySecurity
14 year old Gwen

- Self-taught web designer and developer
- Built websites for local businesses and orgs
- Loved all things Domo
20-something Gwen

- Technical support specialist
- Worked with clients on e-commerce solutions
- Continued honing my craft in design, development, and marketing
30-something Gwen

- Helped design Komand from the ground up as head of UX
- Now a director of UX at Rapid7
- Still loves Domo
I’m not a security expert, but I am responsible for it.
Security is part of the overall experience.
Security is not just the responsibility of the security team
Security vs. UX
Why Security vs. UX?
Another possibility...
DESIGN VS DEV
DEV VS OPS
SALES VS MARKETING
People often think their job function is the most important
Disclaimer: this is not an attack.
How do we move forward and provide security to our users?
Design Principles, Patterns, and Considerations
Layered Information Security

Source: HM Innovation
Design is a mix of requirements, constraints, and tradeoffs.
What works for others may not work for you.
Design Principles, Patterns, and Considerations for Security
Design Principles
PRINCIPLE #1

Know Your User
PRINCIPLE #2

Communicate Goals Clearly
PRINCIPLE #3

Break Down Complexity
PRINCIPLE #4

Design for Trust
Design for Trust

1. Let users feel in control of the experience
2. Be straightforward, and use get personal when you can
3. Use established patterns and remain consistent
4. Prominently display indicators of trust
Design Patterns
Signups, logins, and other easily breached areas
SSL all the things!
PATTERN #2

Email as username?
Password standards

Your password must have:
- At least 8 characters long
- One lowercase character
- One uppercase character
- One number, symbol, or whitespace character

Avoid using a password that you use with other websites or that might be easy for someone else to guess.
PATTERN #4

Make password fields, credit card fields, and similar fields password manager-friendly
PATTERN #5

Don’t collect info if you don’t really need it

Short Forms Outperform Long Forms

<table>
<thead>
<tr>
<th>Short Form (5 fields)</th>
<th>Medium Form (7 fields)</th>
<th>Long Form (9 fields)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversion: <strong>13.4%</strong></td>
<td>Conversion: <strong>12.0%</strong></td>
<td>Conversion: <strong>10.0%</strong></td>
</tr>
<tr>
<td>Cost per: <strong>$31.24</strong></td>
<td>Cost per: <strong>$34.94</strong></td>
<td>Cost per: <strong>$41.90</strong></td>
</tr>
</tbody>
</table>

Source: Marketo
PATTERN #6

Allow users to sign in via OAuth
PATTERN #7

Offer 2-factor authentication as an option

True story: enabling 2-factor authentication on your accounts is actually an act of getting your own raptor gang to protect your logins 🦖จาึก

7:11 PM - 15 Sep 2017
PATTERN #8

Gracefully handle failed login attempts

Your account has been blocked for too many failed login attempts. Username and password do not match or you do not have an account yet.

Use a valid username and password to gain access to the administrator backend.

User Name: admin
Offer a “Remember Me” or “Remember Device” Options
## PATTERN #10

**Offer Role-Based Access Control or Permissions Control in Your App**

<table>
<thead>
<tr>
<th></th>
<th>Publish</th>
<th>Write</th>
<th>Read</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ads</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Blog</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Landing pages</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Website pages</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Social publishing</td>
<td>All accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lists</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
PATTERN #11

Share controls and default share settings
PATTERN #11
Share controls and default share settings

Default to private
PATTERN #11
Share controls and default share settings

Design controls for who can share, who can see, and what they can access.

Share Prototype
The User
Educating the User
“If people find it more annoying to use your measures than not to, they'll do their best to avoid it, which defeats the point of having it.”
We have a responsibility as security companies.
It takes a village.
Questions? Comments? Want to talk more?
Find me on Twitter @gwennasaurus.