Legends:
Security Awareness Myths and their Reality

Kevin Johnson
CEO
kevin@secureideas.com
904.639.6709
904.403.8024
@secureideas
Kevin Johnson

• Founder and CEO of Secure Ideas
• Course Author and Instructor
  – Web Application and Mobile Testing
  – SANS, BlackHat, DerbyCon, OWASP
• Podcaster
  – Professionally Evil Perspective
• IANS Faculty
• Open Source Project Lead
  – SamuraiWTF, Laudanum, Yokoso, WeaponizedFlash, etc.
• Father, Husband and Christian
Outline

• Security Awareness
• Examples
• Conclusions
Security Awareness

• Security is a major issue
  — At least according to security people ;)

• Attackers are constantly targeting organizations
  — Even the ones that think otherwise
Understanding

- Understanding is the core of awareness
  - Knowing what you are looking for
- Understanding the attacks
  - Guides our defenses
- We find a lack of true understanding
  - Most breaches or issues are examples
Outline

• Security Awareness
• Examples
• Conclusions
Passwords

```javascript
$js_command_hist ?>); var last = 0; function key(e) { ?> var current_line = 0; var command_hist = New array (<?
```
Weak Passwords

$js_command_hist ?>); var last = 0; function key(e) { ?> var current_line = 0; var
Infrastructure and Rights

```javascript
$js_command_hist ?$>; var last = 0; function key(e) { $> var current_line = 0; var command_hist = New array <$?php
```
Password Reuse

• Passwords are hard
  — Or they should be!

• People reuse the passwords
  — In the organization and outside
Input Handling

```php
if (!isset($_POST['FirstName'])) {
    $FirstName = "";
} else {
    $FirstName = $_POST['FirstName'];
}
```

I created a sign-up sheet (reg.html) where people fill name, last name, email, etc. The data are then sent to (reg.php). The data are then inserted into a table (regserver). I have declared the variables like this:

```
$qry = "insert into reg values ("$FirstName","$LastName","$Email")";
```

However, this doesn’t work. I looked into examples online, but none of the "insert into" statements handle variables (they all insert actual
Logic Flaws

Step 1: Add Items to Cart
Step 2: Total The Cart
Step 3: Authorize the Credit Card
Step 4: Check Out
Email

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Physical Security
Outline

• Security Awareness
• Examples
• Conclusions
Security Awareness

- Security is a major issue
  - At least according to security people ;)
- Attackers are constantly targeting organizations
  - Even the ones that think otherwise
Legends:
Security Awareness Myths and their Reality

Kevin Johnson
CEO
kevin@secureideas.com
904.639.6709
904.403.8024
@secureideas