Software developers are on the front lines in the battle against malware and hackers. In this presentation you will learn the three primary ways that hackers infiltrate our computers and also the basics of many of the techniques developers need to use to keep them out. We will cover:

SQL Injection

Poor Authentication Techniques

and Cross-Site Scripting

This session is intended for developers that want to learn the basic security concerns they should be aware of when creating applications.

Rob Kraft works at Lucity, Inc. as the Technical Team Lead. He has been developing web applications for fifteen years, non-web applications for thirty years, and spent a few years teaching courses on software development and SQL Server. He often speaks about security in software, particularly related to database products.

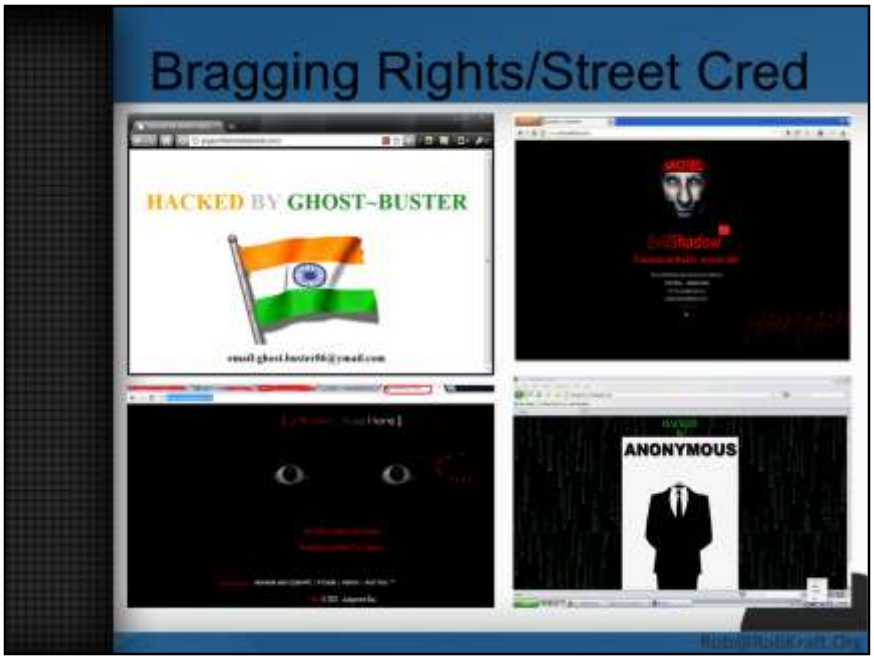

Why Do
They Do It?

MONEY: Bank Accounts. Credit Cards. Amazon Account. Business Fraud. Fraudulent Businesses.

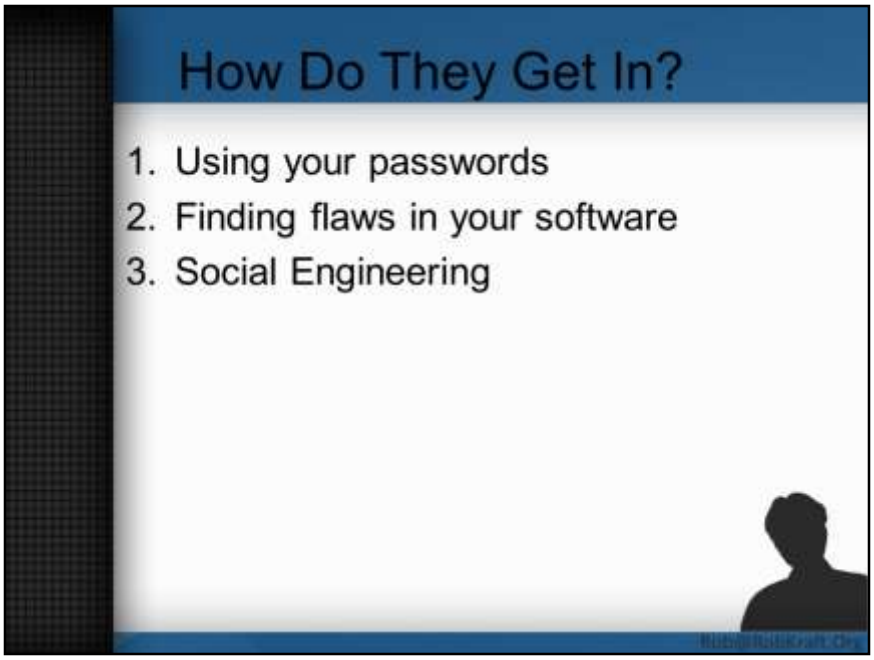
Your Disk Space. Story of my client that had server slow down due to video/music sharing installed by hackers. Your CPU, for bitcoin mining and for probing other computers on the Internet. They could install web servers and email servers on your computer and use them for nefarious purposes. Law enforcement will find you and prevent your computer from getting on the Internet, not the hackers machines.

Enlist your machine in their zombie army. Botnet. Botnets are hundreds or thousands of computers running a “bot” that is waiting to be sent commands. Those commands usually instruct the bots to launch attacks on other computers, often attempting to perform a distributed denial of service attack to flood the target computers with so many requests that they have to go offline.

Destruction: State Actors, Anonymous. LulzSec. In cyberwar, hackers simply want to damage the ability of their enemies to use their computers and information systems.



Deface Sites for Bragging Rights. Many hackers need to make a name for themselves so they can sell their skills on the dark web and make money.



I grouped the attacks into three broad categories for this presentation. Each will be covered in more detail.

Logging in with stolen logons and passwords is probably the least used of the three methods of gaining access.

Passwords to individual accounts are sought after to gain access, usually for just a short time until they are discovered, to use someone's personal finances. If you are a VIP, hackers may seek to embarrass and harass you.

Administrator Passwords are usually more valuable than user passwords because they provide access to an entire server and likely all the servers, data, and information within a company. Skilled hackers sometimes use stolen admin passwords within companies for months stealing data before they are detected.

Hacking is highly automated. Only rarely would a human be sitting at a computer attempting to get in by guessing passwords. Instead, programs are launched to run all day and all week long making attempts at logging in with different passwords.

Any information that is in the browser should not be considered secure because if the page/site has a malicious javascript infection, hackers can read any of that information. Writing code to keep secrets hidden from the person sitting at the web page and using it does not hide those secrets from the javascript. The server should validate all data coming in to it when it receives it. The server code should never trust what the browser sends to it.

Basic Authentication, the original technique for sending passwords from the browser to the server, does not hide the password, it simply encodes it and hackers can easily decode it with a base64decoder and see the values. Encoding is used to prevent special characters like ampersands and semicolons and spaces, that people may put in their passwords, from confusing the programs reading the values because they think the special character signifies the end of the value.

If your page has sensitive data, don't allow it to run inside an Iframe (add a header that says X-FRAME-OPTIONS: DENY).

Use a 3rd party system for passwords. Have your users log in with their facebook or google account. If you want more control over the user accounts use a service like Auth0 or Okta. Place the risk of password protection onto these 3rd party systems that are experts at it and that provide multi factor authentication, password resets, and strong password policies.

If you are providing your own password page, don't allow any javascript to run on the page.

Use HTTPS for all sensitive data. That is the only way to protect the values entered from "Man In The Middle" (MITM) attacks that could occur when any server between the web page and your web server passes the data along the Internet. HTTPS means the data gets encrypted in the browser and is not decrypted until it reaches your server.

Support Multi Factor Authentication to guarantee people logging in are who they claim to be. This is often done by sending them a text message when they attempt to log in.

These rules should apply to any sensitive data you need to collect, such as credit cards. Rule #1 is to outsource this task to some other site that specializes in it.

Allow paste into password fields so that people can use password managers effectively.

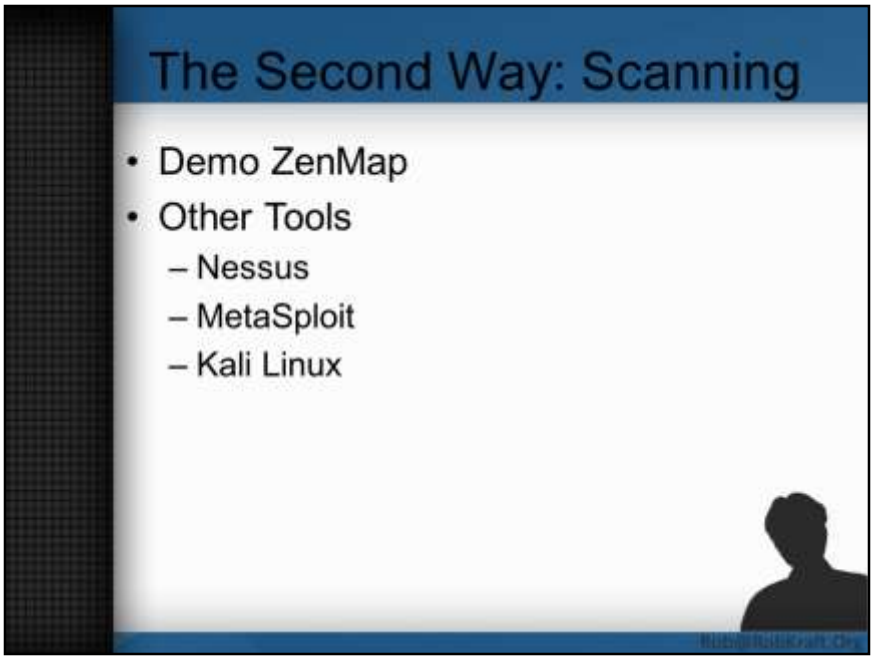
Allow the browser/app to have an option to show the password the user is typing. Hiding the password only hides it from other humans peering over the shoulder of the person entering the password. Hiding the password does nothing to prevent its visibility from malicious software.

Nothing From the Browser is Safe!

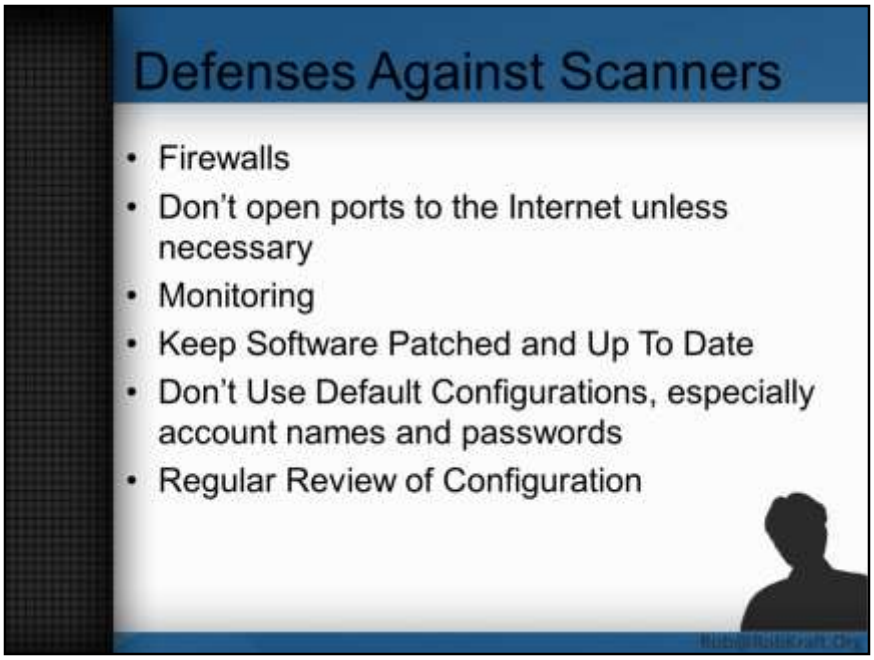
- The server should never trust data sent to it from the browser/client
  - Code (Javascript) in the browser could check a user's permission before allowing the user to delete data, but a hacker can easily alter that javascript to allow the action.

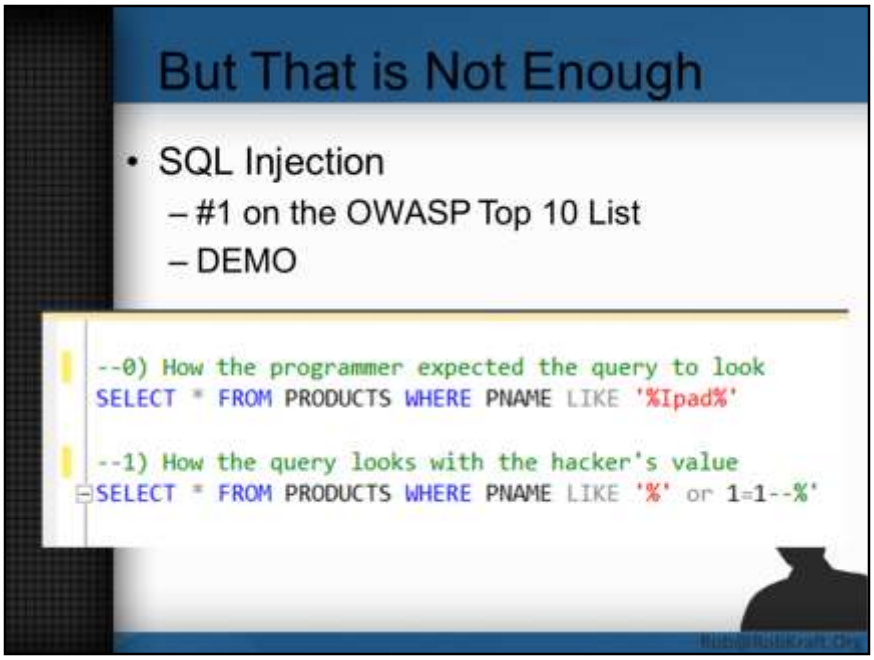
Databases with Passwords in them, or the backups of databases with passwords; are a treasure trove for hackers. Not only do they allow the hacker to find the logon ID and password of a user, they often can use the same credential for that user on other sites!

Use a 3rd party service like Auth0 or Okta to store passwords. They are experts at it. If you are doing it yourself, make sure you pick a strong algorithm like Bcrypt. Never try to write your own encryption because hackers can easily break it mathematically. Require strong, long passwords. Allow copy/paste in password fields so that Password Managers work; if you don't users will pick the simplest passwords they can because they don't want to type the long complicated passwords that Password Managers can provide.



Hackers have a lot of tools for penetrating networks. These tools are used by both bad guys and good guys. Good guys use them to find flaws so that they an be fixed. Kali Linux is a free Linux OS full of tools for hacking. Metasploit is a popular tool for exploiting vulnerabilities. Many tools exist that get automatic updates that allow hackers to break into systems without even understanding how the hacks work.

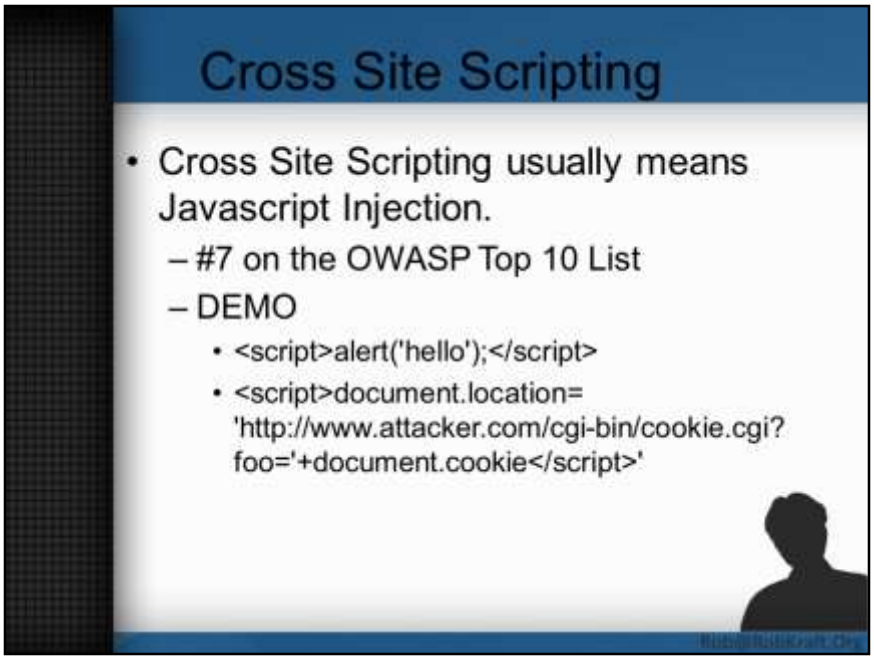

Defenses Against Scanners
• Firewalls
• Don't open ports to the Internet unless necessary
• Monitoring
• Keep Software Patched and Up To Date
• Don't Use Default Configurations, especially account names and passwords
• Regular Review of Configuration



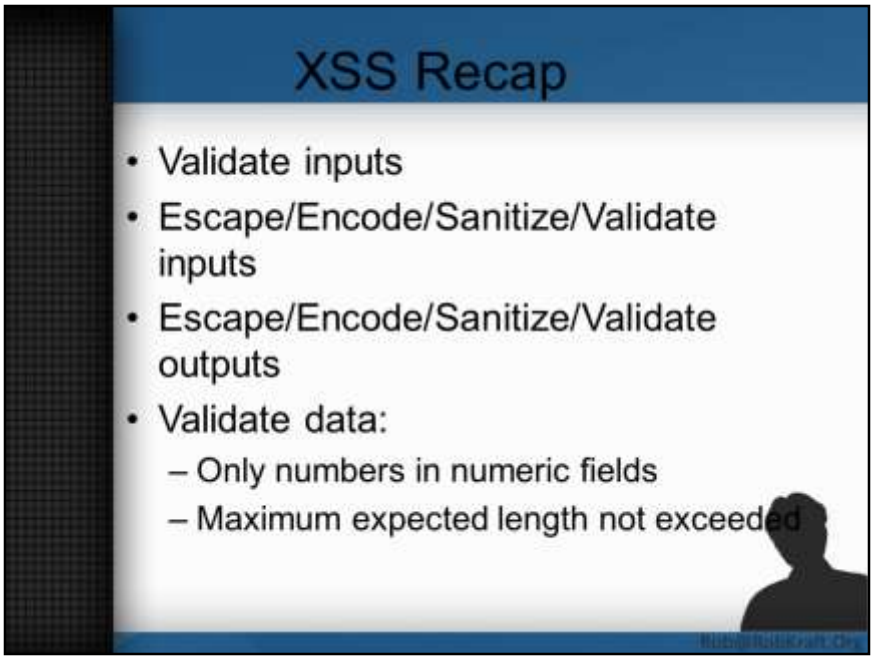
No firewalls can be relied upon to block all hackers ingenious attacks. Developers need to protect against SQL Injection. The Internet if full of resources for protection. I recommend looking at OWASP.ORG. Basically, all dynamically built SQL should be evaluated for sql injection risk. Single quotes to need to be “escaped”. 1) Use “procedures” instead of dynamically building SQL to reduce risk. 2) Write a function called EncloseInQuotes and pass all dynamically constructed SQL variables through that function.

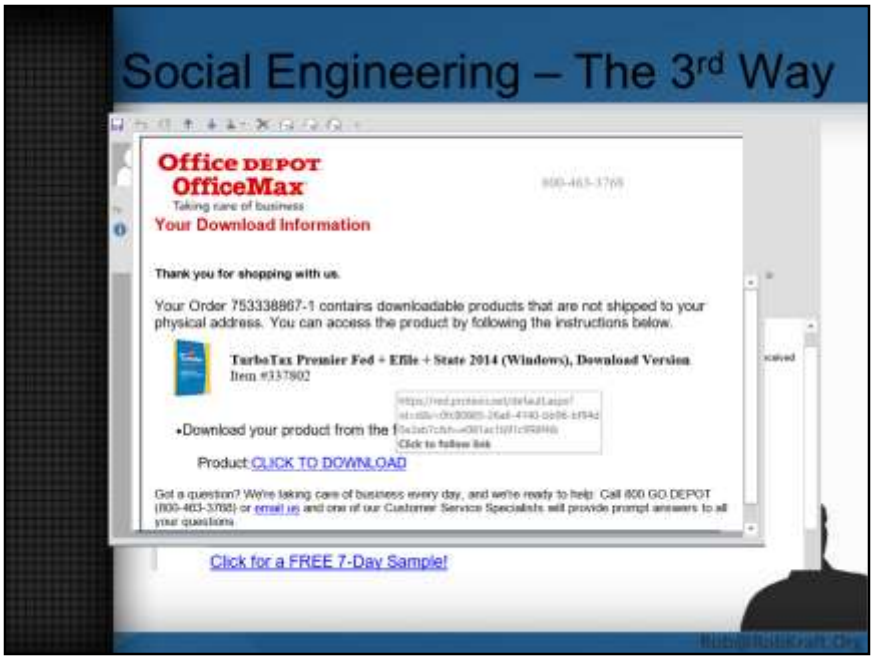
SQL Injection Recap

- SQL Injection works because our programs construct commands in the SQL language to send to the database to tell it what to do.
- Hackers alter the commands we construct to tell the database to do things they want to do.
- This may allow them to delete data, access the operating system, or all computers in your company!

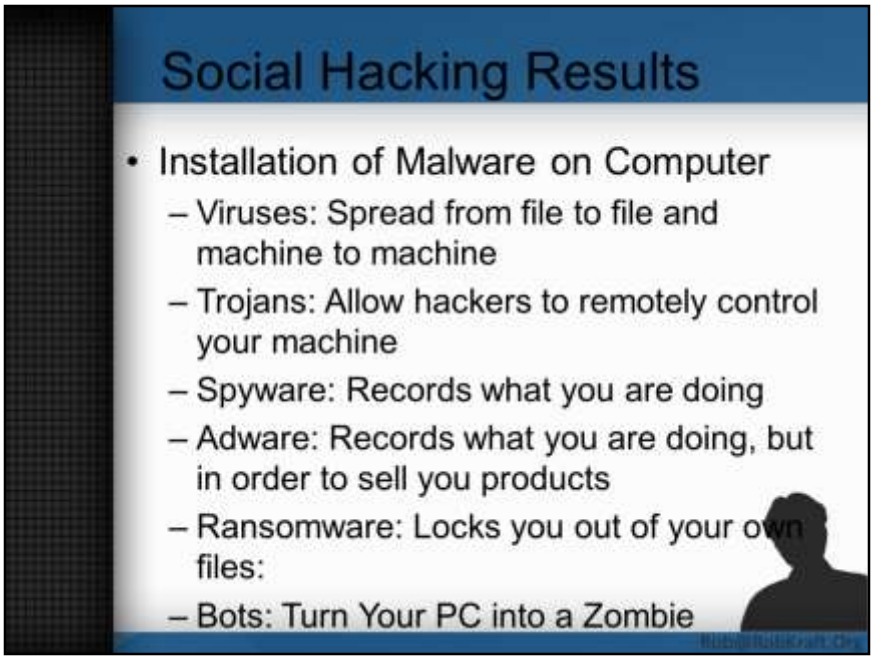


Cross Site Scripting (XSS) – Needs to be blocked by “escaping” all user input, as well as any dynamic content coming from a database to a web page. Each programming language has different tools for “escaping” the javascript to prevent it from running.


XSS Recap
• Validate inputs
• Escape/Encode/Sanitize/Validate inputs
• Escape/Encode/Sanitize/Validate outputs
• Validate data:
– Only numbers in numeric fields
– Maximum expected length not exceeded

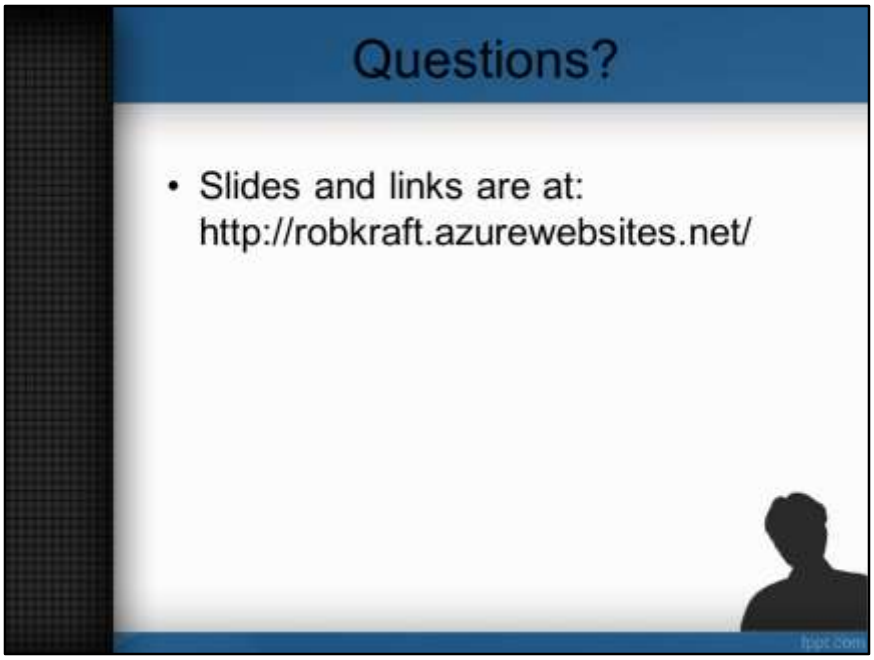


Hackers send emails that attempt to lure people into clicking on links that will install malware. Hackers often also attempt to lure people to their web sites using "clickbait", which are usually ads on web pages that temp people to click on them. Clickbait is often not malicious too. The majority of clickbait just wants you to navigate to a new page because they collect ad revenue for every page view.



Social engineering is used to install many types of malware on computers.

Services like KnowBe4.com can train your users to not click on links in emails.


Questions?
• Slides and links are at:
http://robkraft.azurewebsites.net/

Links From Presentation

- https://info.varonis.com/web-5ve-webinar-identify-ransomware-en/nam webinar 2/21
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  - Great PDF of top 10 - how to defend in many programming languages
- https://www.kansascityusergroups.com
  - OWASP KC - https://www.owasp.org/index.php/Kansas_City
  - 04/20 - 04/21 - BSides KC Security Conference (https://www.bsideskc.org/)
  - 07/11 - 07/13 - Kansas City Developer Conference KCDC (http://www.kcdc.info)
- Using Bcrypt in C#:
  https://www.codeproject.com/Articles/475262/UseplusBCryptplustoplusHashplusYourplusPasswords
- https://asafaweb.com/ - Free scan of your .Net Web Sites for risks
- https://securityheaders.io/ - Get a score of the HTTP Headers sent by your site
- https://content-security-policy.com/browser-test/ - Test your browser's CSP
- https://www.ssllabs.com/ - Test your Server or Browser
- http://webkay.robinlinus.com/ - What your browser knows about you
- https://www.f-secure.com/en_US/web/home_us/router-checker - Check your router
- https://haveibeenpwned.com/ - Is your email in a major breach?
- http://map.norsecorp.com/#/ - A live map of attacks going on around the world
- https://cybermap.kaspersky.com/ - Another live map of attacks around the world
- https://www.malwarebytes.com/remediationmap/ - Global map of malware getting cleaned up
- https://auth0.com – Provides identity management (User accounts and passwords)
- https://okta.com - – Provides identity management (User accounts and passwords)
- Facebook, Microsoft, Google – All offer OAuth Identity Management
- https://www.thinktecture.com/identityserver/ - Free, open source Identity Management tool w
  We use this at Lucity

Links From Presentation

- http://www.routerpasswords.com/
- https://datarecovery.com/rd/default-passwords/
- https://www.kali.org/ - Kali Linux Free OS full of Hacking Tools
- https://www.cloudflare.com Free HTTPS for personal sites
- https://lastpass.com – Great password manager
- https://keepass.info/ - Greate password manager
- https://www.knowbe4.com/ - Provides businesses inexpensive social engineering education
- https://nmap.org/zenmap/ - Zenmap – tool for probing ports on any computer
- https://www.metasploit.com/ - Metasploit – very popular tool for penetration testing
- https://www.tenable.com/products/nessus/nessus-professional - Nessus Network Scanner
- https://www.keycdn.com/blog/x-xss-protection/
- https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/
- Google: How to Prevent Cross-Site Scripting Attacks
- Google: How to Prevent SQL Injection Attacks
- Excellent Free Course on Pluralsight: https://app.pluralsight.com/library/courses/hack-yourself-first/table-of-contents

Links From Presentation

- 7 Short Videos of Basic Security Measures for End Users To Protect Themselves from Hackers:
  - https://www.youtube.com/playlist?list=PLYEr6kVanyrPu1gZ5g6iOr0v4ImpOOCSH
- A Free One Hour Course That Teaches How The Most Common Hacks Work
  - https://www.varonis.com/learn/web-security-fundamentals/
- A Free One Hour Course on Ransomware
  - https://www.varonis.com/learn/introduction-to-ransomware/
- Policies for Protecting Passwords:
  - https://en.wikipedia.org/wiki/Password_policy
- How To Make Your Own Passwords Strong:
  - https://www.privacyrights.org/blog/10-rules-creating-hacker-resistant-password
- Popular Tools Used For Hacking: http://sectools.org/