The Secure Business Workshop

- Presenter: Tom Germain
- Sponsor: Coder Scoop Inc.

What techniques do they use?

- DDOS
- Phishing (email)
- Malware
- Worms
- Trojans (software,USB mems)
- Social engineering
- Click bait

Definitions (Google them!):

- Botnet
- Juicy target
- Vulnerability
- Exploit
- Script kiddie
- Ransomware
- Spoofing
- Zero day
- Root kit

The best ways to make yourself more vulnerable...

- Don't patch your O/S, software
- Use easy-peasy passwords
- Use public WI-FI anywhere
- Use http instead of https
- Use ftp instead of sftp
- Use telnet instead of ssh (!!!)
- Visit lesser known web sites
- Click links / open attachments in emails
- Use older, non-supported versions of Windows
- Use IOT devices
- Don't use an anti-virus / firewall / ant-malware
- Put stuff online that you wouldn't want your mother to see
- Dispense your private information like candy

What does a good/bad password look like?

- Password123 : BAD
- 19891012 : BAD
- 05@86We57# : GOOD

How do Websites get hacked?

- Weak passwords
- SQL injection
- XSS (Cross-site Scripting)
- XSRF (Cross-site request forgery)
- Vulnerabilities in web app used
- Vulnerabilities in plugins
- Vulnerabilities in web server

A word about Wordpress

- Favorite target for hackers
- In a Sucuri study 78% of hacked sites used WP
- Vulnerable design
- Plugins and themes often badly coded
- Use Wordfence or Sucuri plugin or both
- Don't use newer or unmaintained plugins
- Disable comments or at least moderate them

Sources of info on vulnerabilities

- Krebs on security: https://krebsonsecurity.com/
- Wordfence blog: https://www.wordfence.com/blog/
- National vuln. Database : https://nvd.nist.gov/
- Live map: https://map.norsecorp.com/
- US-Cert : https://www.us-cert.gov/ncas

The Obvious

- Use long, **random** passwords
- Make every password **unique**
- Don't install dodgy apps
- Treat every email with suspicion – they're easily forged
- Use Gmail or similar
- Use VPN for Wi-Fi
- Educate others who might use your devices
- At work, be weary of calls from people you don't know

Am I a victim?

- Was my user account hacked / data stolen?:

https://haveibeenpwned.com/

- Has my website been hacked? [not on sheet]

https://sitecheck.sucuri.net/

https://quttera.com/website-malware-scanner

Test your router / provider

Check router for misfortune cookie:
https://www.wordfence.com/blog/2017/04/check-your-router/

Check router https://campaigns.f-secure.com/router-checker/en_global/

Check dns servers for spoofability:
https://www.grc.com/dns/dns.htm

Check telnet port, a hacker fav:
https://www.grc.com/x/portprobe=23

What's two factor authentication?

Use an additional method of verification, such as a knowledge question: “what's your mother's middle name”

VPN Services

- ❑ https://ca.norton.com/wifi-privacy
- ❑ https://www.hotspotshield.com/
- ❑ https://www.ipvanish.com/
- ❑ https://nordvpn.com/
- ❑ https://www.vpnunlimitedapp.com/

What's a Firewall?

Software and/or hardware that controls Internet traffic at the “gate”

- Ex: Windows Defender
- Alternative, Free for PCs: ZoneAlarm
- Lan: Juniper
- Linux: iptables

To participate in our many other workshops: https://coderscoop.com/events