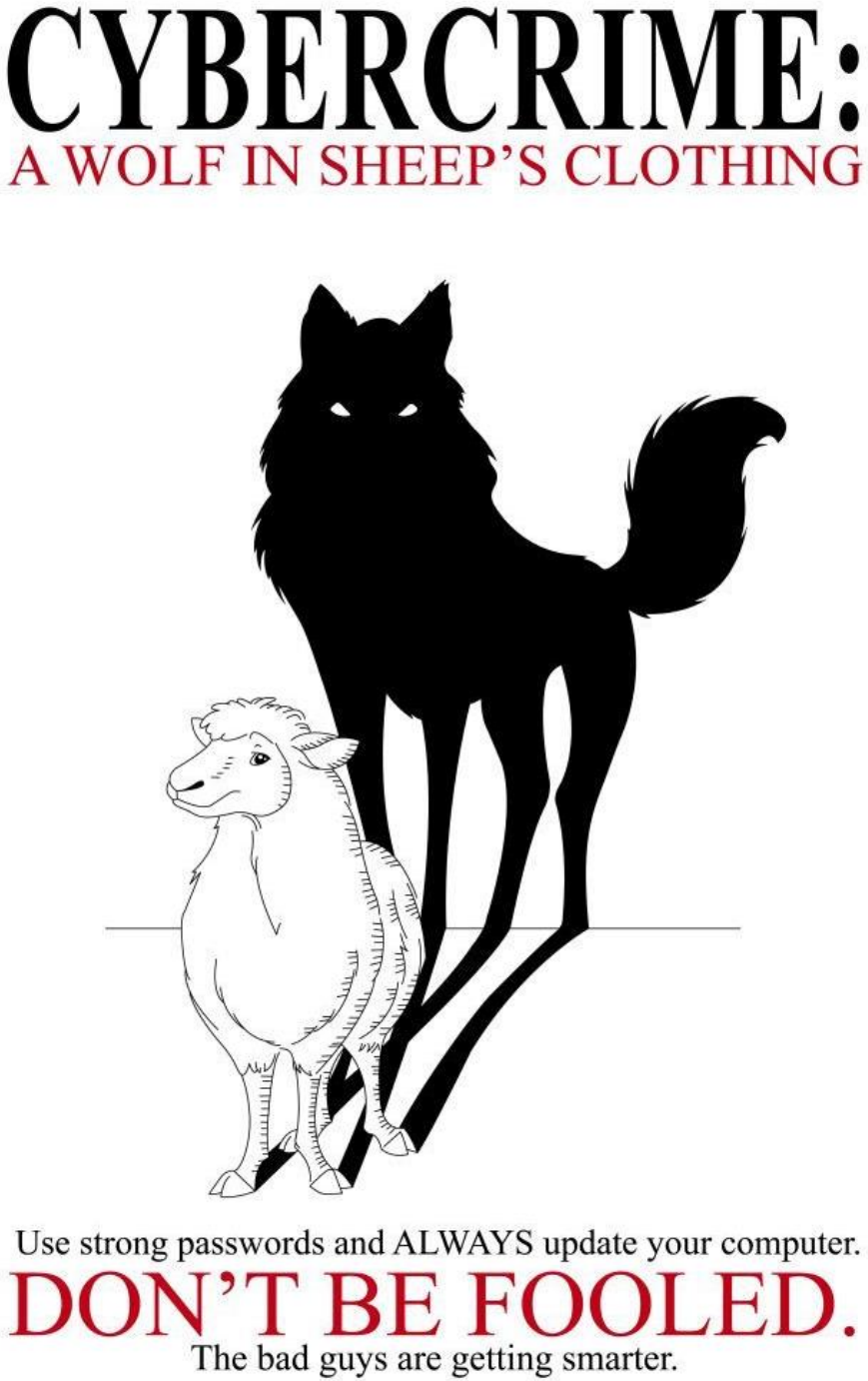


"Staying Safe Everywhere"

- Corporate Intranet Safety
- Working from Home – Staying Safe
- Staying safe online – Everywhere
- How do we protect ourselves everywhere ?
- Social Engineering, a quick overview

Presenter: Susi du Preez

Corporate Intranet Safety

What is an Intranet?

5 Ways to stay safe on your Intranet

1. Ensure the system is pin/password protected
2. Monitor users who login
3. Restrict Access to the most sensitive information
4. Create Intranet Usage Policies
5. Regularly review & update the information

Staying safe – Working from Home →

This applies to working safely from anywhere

- Keep your passwords to yourself
- Ensure up-to-date security protection is in place
- Look out for Phishing emails
- Use a VPN when working away from the office
- Use MFA (multi factor authentication)
- Latest Updates
- Anti Virus
- Router Security

Staying safe online --EVERYWHERE

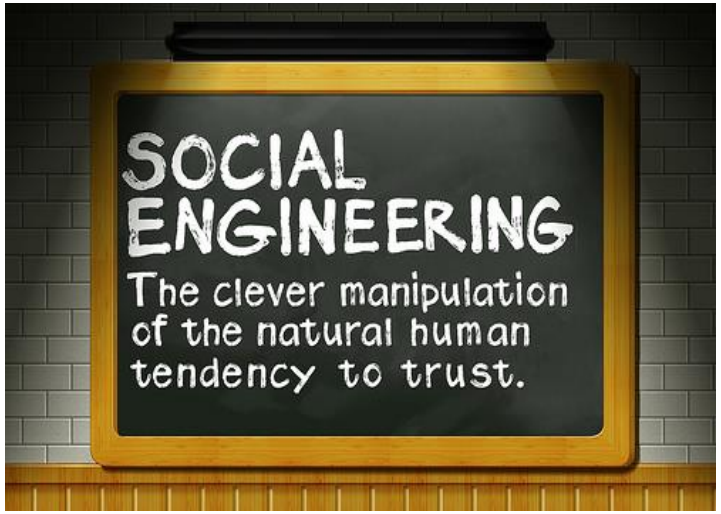
10 Tips to staying safe online

1. Create complex passwords
2. Boost Network Security
3. Use a Firewall
4. Click Smart – Think before you click
5. Be a Selective Sharer
6. Protect your mobile devices
7. Practice safe surfing/shopping
8. Keep up to date
9. Lookout for scams
10. Keep your Guard up & backup, backup and backup more…

What can I use to protect myself?

- Awareness is the number one defensive measure.
- Be aware that social engineering exists and be familiar with the most commonly used tactics.
- Test and Train your staff and retrain them often
- Train and make your staff aware that these practises have to be implemented **both at work and in everyday life** even at home
- Criminals will go to any length to get what they want, there is no boundary for them, criminals follow a different set of rules than the rest of us!

Social Engineering – a quick overview

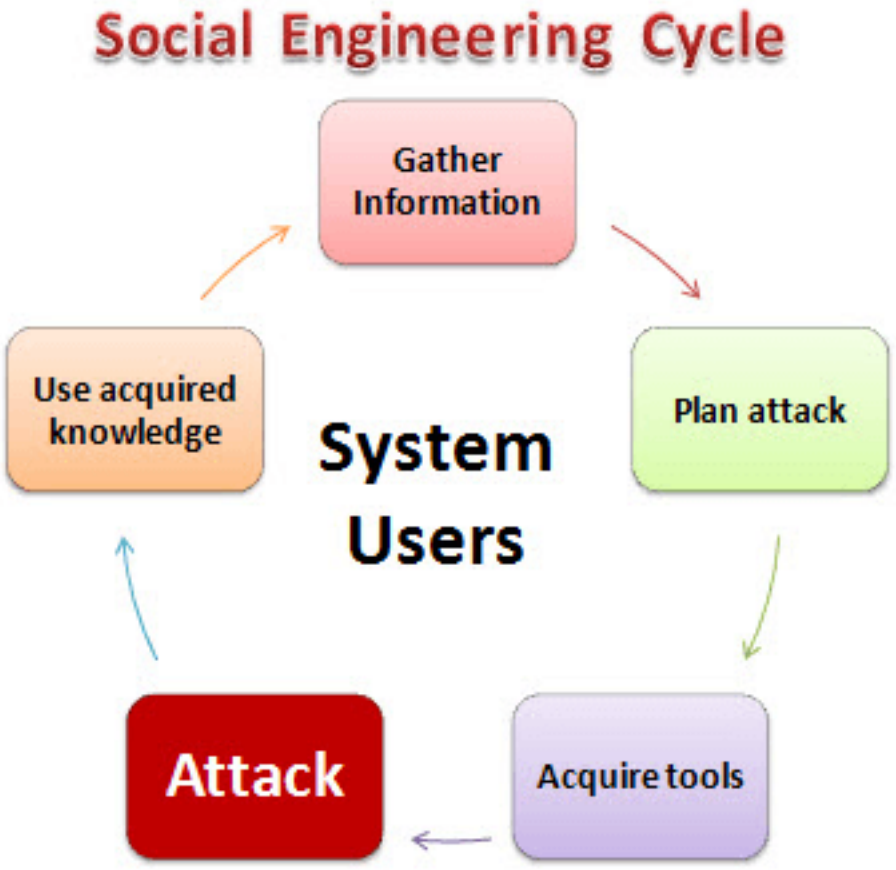


What is Social Engineering?

REMEMBER by the time you are being subjected to a social engineering attack, you have already been researched thoroughly and they know just about everything about you already

The 4 phases of the Social Engineering Cycle:

- **Information Gathering** – collecting information to help identify attack vectors and targets.
- **Relationship Development** – develop a trust relationship with the target.
- **Exploitation** - Use information and relationships to infiltrate the target.
- **Execution** – Accomplish ultimate goal.



Q & A

www.impactit.co.za

www.netwrm.com

https://twitter.com/netwrm

https://www.linkedin.com/in/netwrm/

Feel free to contact me on any of the links on this page