Watering Hole Attacks

A basic safety guide

Recognizing the signs

1. Unsolicited notifications, such as:
    - “trusted” sites asking you to install or agree to the use of software never mentioned before
    - frequent alerts for software updates that won’t seem to stop
    - a lot of pop-up advertisements

2. Changes:
    - unwanted changes made to your browser settings
    - changes made to your computer settings
    - sudden lack of storage space

3. Speed:
    - the computer suddenly slowing down
    - notice many services running that you have never seen or heard of

Preventing an attack

1. Practice online safety:
    - stick to sites that start with https, with the ‘s’ standing for “secure”
    - consider anti-malware software to keep you safe online, most will recognize a malicious digital signature on downloadable files or websites
    - don’t click on links you do not recognize or are not expecting to receive
    - don’t talk to strangers, verify explicitly

2. Keep your computer systems up to date:
    - Keep patch management processes up to date, patches are often protecting against exploits
    - Ensure your identity lifecycle management is up to date, remove employees that no longer work there
    - Ensure firewalls and anti-malware software is up to date, they contain digital vaccinations that should recognize more recent malicious signatures

3. Think defense in depth:
    - Use firewalls, they may protect you against malicious downloads
    - Monitor internet traffic with anti-malware software
    - Disable insecure internet access (e.g. don’t allow http, only https)
    - Run periodic diagnostic scans, this can be set up to run automatically and alert you to anything untoward
    - Provide staff training, forewarned is forearmed