★ 7 WAYS HACKERS LOOK TO ★

EXPLOIT

YOUR STATE AND LOCAL GOVERNMENTS

#1 HUMAN ERROR

Don't get lax on protocols and rules put in place to keep you and your organization safe.

Implement security awareness training as well as mandatory security protocols like frequent password resets.

#2 YOUR PASSWORD

Don't have one key for all of the doors you can open.

Instead, have many passwords, change them routinely and don't use information that can be easily found through an online search.

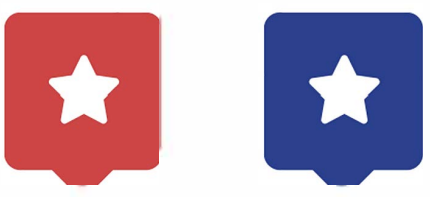
#3 PHISHING ATTACKS

It really is as easy as downloading a file that looks like it's from a coworker or clicking on a link that you think your friend sent you.

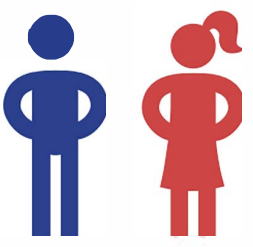
Train your staff to be wary of any and all communication they received and test their awareness consistently.

#4 Application and Software Bugs

Devices **Applications**



There are various applications and devices that you and your team need to use on a daily basis to get the job done. Often, bad actors already know the weak points in these systems, especially if they have exploits and patches that have been available for a while.



How to Test and Secure:

It's vital to continuously monitor and apply software patches to your programs and update your anti-virus software. You should also be running frequent penetration-tests on your network to ensure the software patches are working and find any other vulnerabilities.

#5 Social Engineering

YOUR INFORMATION

Your Facebok, Twitter and LinkedIn information

BAD ACTORS

Attackers looking for ways to steal your credentials

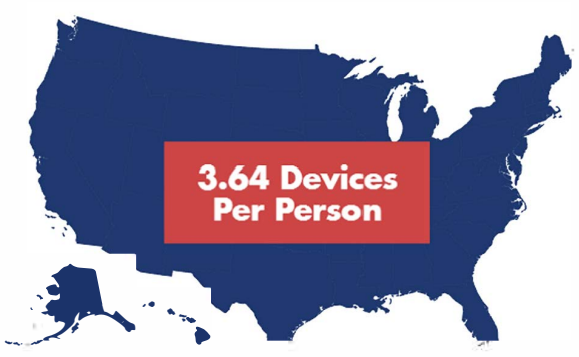
If you use personal information as a password or a clue to reset your password, you could be at risk for a social engineering attack. Make sure that your organization uses multi-factor authentication for all password resets and train your staff not to use any information they may share online as part of their security.

#6 DDoS Attacks

The problem is multifaceted – but one of the main drivers for this attack is that we have so many embedded devices on our networks that are often overlooked from a security perspective which is a fact that our adversaries are taking advantage of.

Being able to quickly detect compromises on the network and understanding the attack path to the critical assets can help you prioritize the vulnerabilities to fix and quickly take action on the right resources before something bad could happen. The best defense here is a good offense by knowing where you are vulnerable to these type of attacks and knowing where to patch and protect as much before they start.

#7 Personal Devices



The average number of personal devices per person continues to grow which means if you don't have a Bring Your Own Device (BYOD) program - now is the time to start.

Remember, while it may be convenient to instantly connect to networks or search for open WiFi locations it is incredibly dangerous for your device and the future networks you connect to. Attackers may create fake WiFi connections or use the "Man in the Middle" approach to obtain your password information for your device.

At the end of the day, we know that attackers are out there and that breaches will happen. Know that the bad actors out there are one step away from reaching sensitive data and that you should be well versed on what you can do to protect your government agency and the communities you are serving. Having a strong understanding of what your current IT environment looks like and what vulnerabilities are high priorities for your organization is crucial towards your organization's security posture. Consider speaking with one of our security consultants about Core Impact or our security consulting services, today!

For more information, visit www.coresecurity.com.

CORE SECURITY