UTC ISP
32 Street Lane
Earley
Reading
Berkshire

Phone: 123-456-7890
Fax: 123-456-7890
E-mail: isp@utcreading.org.uk

# Knowing Your Threats: A Leaflet by UTCISP

## Who are we?

We are UTCISP, a small ISP with most of our customers based in and around the Reading area. We have created this leaflet to help you, our community, understand the threats that can affect your computers, laptops and other devices. We want you to get the most out of life, and you don't need some hacker stealing all your data.

Consider switching to our network for the most secure connections.



# Learn More

To learn more about Threats pertaining to our systems and how we fix them, visit isp.utcreading.org.uk. Feel free to also send an email to ISP@UTCREADING.ORG.UK for more information about this topic.

This leaflet/brochure was designed by Nathan Windisch, a junior IT consultant. For any feedback about this leaflet/brochure, email me at NATHAN.WINDISCH@UTCREADING.ORG.UK

# EXTERNAL MALWARE ATTACKS

One threat to the computer system in our organization is malware attacks. Malware attacks can be issued to the system externally, via FTP, SSH or even email. Malware attacks are very dangerous and can cause lots of damage of let into our system. Given that we are an Internet Service Provider it would be catastrophic if malware were to get sent into the system as many people who use our systems could be infected, resulting in mass loss of data and a subsequent loss of profits due to customers cancelling their contracts with us as there has been a data breach, resulting in a loss of trust.

## Phishing

Phishing is a way that scammers can gain access to data owned by either a business or a private person or people. Phishing can be very effective towards individuals who trust official looking documents, even if they are not legitimate. All emails should be scanned to see if they are from an official source before any attachment is opened or any link is clicked. If an email is found to be possibly malicious, the IT team should be notified immediately. This can be detrimental to our industry as if a phishing email is sent from an official email, many customers may be affected by it, leading to a loss of trust and profits.

## DOS/DDoS

A DoS attack, or Denial of Service attack, is a way to slow down or stop the victim's internet connection by sending lots of packets of data towards the target, resulting in the connection being interrupted due to legitimate packets not being able to access the network. A DDoS attack, or Distributed Denial of Service attack, is a more powerful version of a DoS attack but, given that it is Distributed, it is much harder to stop. With a DoS attack, the packets can be blocked by denying the IP address of the attacker. With a DDoS attack, however, the packets are being sent are from multiple sources, normally gained from a BotNet. The resultant attack is hard to block without disabling access to legitimate outside users. DDoS attacks can result in downtime, meaning that our users may stop using our services.

## BotNets

A BotNet is a way that hackers gain access to multiple computers to perform attacks. BotNets creators can use tactics such as Malware Attacks and Phishing to gain access to the user's system. Once they gain access, they can use the computer as a 'slave', using it to do things using their internet connection to perform things like DDoS attacks, as aforementioned, or using their processing power to perform things such as brute-forcing or bitcoin mining. BotNets can mean that our users lose trust in our services and move over to an ISP.