Intercontinental Trust Ltd

April 2020

INSIDE THE HACKER'S MIND
SOCIAL ENGINEERING FRAUDS & SCAMS

INTERCONTINENTAL TRUST LTD (ITL)
www.intercontinentaltrust.com

CYBER THREATS

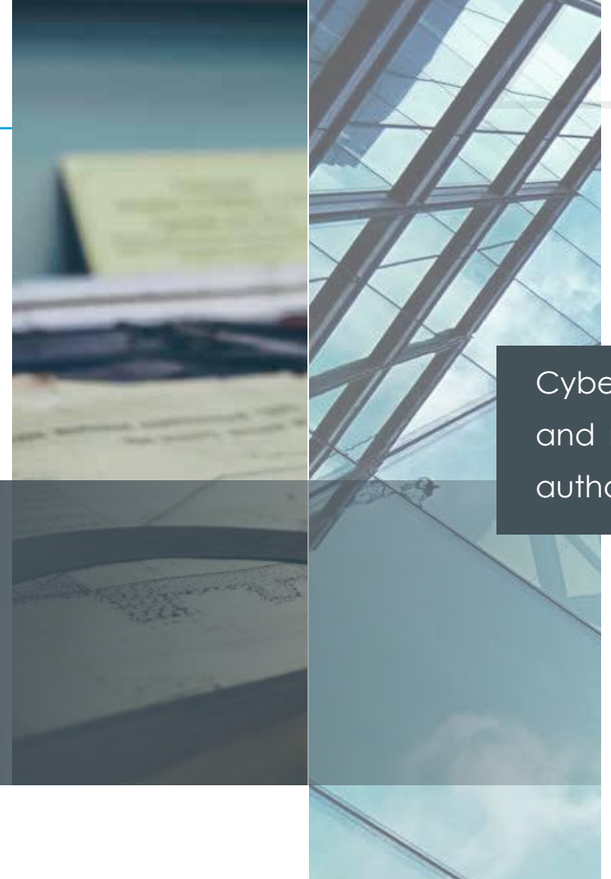
THE ART OF HUMAN HACKING:
SOCIAL ENGINEERING

63% of social engineering attacks are successful and is recognized as one of the greatest and ongoing cybersecurity threats for organizations across the world
– The ITL Information Security Team 2020

Social engineering relies heavily on human interaction and often involves tricking end-users into breaking standard security practices.

Types of social engineering attacks:

1. Baiting
2. Phishing
3. Vishing (and Pretexting)
4. Quid Pro Quo
5. Spear Phishing



Fraudster's Hacking Techniques

Cybercriminals masquerade their real identities as trusted sources and manipulate their potential victims in order to gain legitimate, authorized access to confidential information.

Fraudsters can call you from what looks a genuine phone or mobile number.

Fraudsters may keep landline open by not hanging up and even play a dialing tone over the phone.

Fraudsters can send SMS requesting you to call them or click on a link.
These SMS may usually appear in the same text thread as genuine messages.

Fraudsters can send you malicious URLs via emails which when clicked upon, can steal your data, infect or take control of your devices.

BAITING and QUID PRO QUO

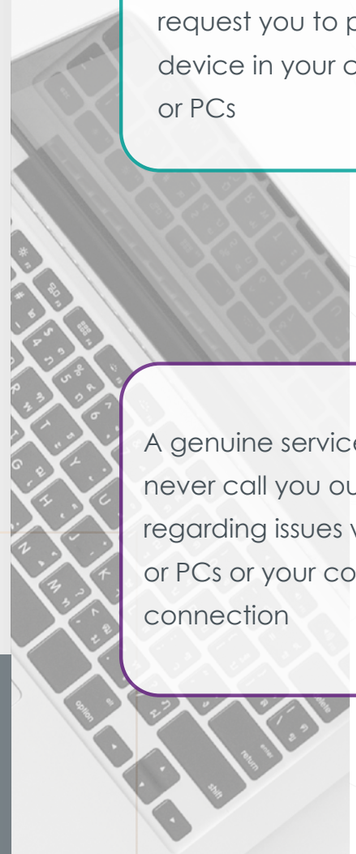
THE CLAIM

Hackers may approach you as trusted IT service providers of your organisation and claim to have to troubleshoot your endpoints by giving you a malware infected device, such as a USB removable media or CD or leave the media containing the malware in a place where you will likely find it.

A quid pro quo attack occurs when attackers request private information from someone in exchange for something desirable or some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift.

THE SCAM

The success of a baiting attacks hinges on the notion that the person who received or find the infected device will load it into their computer and unknowingly install the malware. Once installed, the malware allows the attacker to advance into the victim's system.



Protect yourself

Never accept money or any forms of gifts from strangers that request you to plug any external device in your corporate laptops or PCs

A genuine service provider will never call you out of the blue regarding issues with your laptops or PCs or your corporate Internet connection

Do not plug in any removable medias that you find around and do not know to whom it belongs

Do not click on any download URLs that may have been provided by the caller

Inform the relevant cyber-security authorities should you find yourself in a baiting situation

PHISHING & SPEAR PHISHING

THE CLAIM

Phishing occurs when an attacker makes fraudulent communications with a victim that are disguised as legitimate, often claiming or seeming to be from a trusted source. The most favoured approach of phishing is via email.

Spear phishing is a highly targeted type of phishing attack that focuses on a specific individual or organization. Spear phishing attacks use personal information that is specific to the recipient in order to gain trust and appear more legitimate.

THE SCAM

In a phishing attack the recipient is tricked into clicking a malicious URL or sharing personal, financial, or business information by exploiting the ignorance of end-users.

Email is the most popular mode of communication for phishing attacks, but phishing may also utilize chat applications, social media, phone calls, or spoofed websites designed to look legitimate whereby hackers will explicitly force you to login.

Protect yourself

- If the sender is not known, be more vigilant and pay further attention
- Check for misspelled words in the request
- Be wary of threats and urgent deadlines – Do not act blindly or in haste that you ignore warning signs
- Do not click on suspected or suspicious URLs inside attachment from mails
- Do not download attachment from mails you have suspicions on or you don't know the sender
- Follow established procedures and guidelines in place for all transactions
- Continuously raise your cyber security awareness

VISHING (and PRETEXTING)

THE CLAIM

Vishing (voice or VoIP phishing) is the voice version of email phishing. Here, instead of conducting the phishing attack through email, it's conducted using the voice medium. Hacker may call you via what you may think is a genuine phone or mobile number and impersonate trusted sources. They will insist that they are here to help you.

Pretexting occurs when an attacker fabricates false circumstance to compel a victim into providing access to sensitive data or protected systems.

THE SCAM

Vishing is a phone scam in which individuals are tricked or scared into handing over valuable financial or personal information to scammers.

Examples of pretexting attacks include a scammer pretending to need financial data in order to confirm the identity of the recipient or masquerading as a trusted entity such as a member of the company's IT department in order to trick the victim into divulging login credentials or granting computer access.

Protect yourself

- Never give personal information over the phone to caller you cannot genuinely identify who they are and what their real intentions are
- Hang up, look for the number of the company on their website, and call them directly to make sure it was a legitimate call and request
- In case you identify the call as a potential vishing attack, politely hang up the call and inform the concerned cyber security authorities

Reporting

If you have fallen victim to cybercrime, kindly seek assistance from your Information Security Team and cybercrime agencies or authorities of your country. Reporting mechanisms vary from one country to another. In Member States which do not have a dedicated online option in place, you are advised to go to your local police station to lodge a complaint.

In Mauritius, we have The Mauritian Cybercrime Online Reporting System (MAUCORS) which is a national online system that allows the public to report cybercrimes occurring on social media securely. It will also provide advice to help in recognizing and avoid common types of cybercrime which takes place on social media websites.

Contact us

The financial services landscape is undergoing a wave of innovation thanks to disruptive technologies and service providers are embracing digital transformation in response to the ever-evolving needs of their customer base. But innovation surely presents new risks; with hordes of cyber-attackers waiting to pounce on security loopholes, it is important that there is a solid cyber security strategy in place.

Globally, cyber threats are growing across industries and sectors; all industries are impacted and we, as organisations, need to be always ready for war against hackers.

Recent surveys from global security institutions also demonstrate that many organisations are struggling to protect their infrastructure adequately and this corroborates with the predictions that cybercrime will cost the world USD 6 trillion annually by 2021.

Cybersecurity is firmly entrenched in our company strategy and for that reason, we have set up a full-fledged IT, Information Security, Governance, Risk & Compliance, and Data Protection team with expert knowledge in various technological areas.

If you want us to assist you in establishing a mature IT infrastructure & Information Cybersecurity strategy, please feel free to contact us at:

info@intercontinentaltrust.com
(+230) 403 0800
https://intercontinentaltrust.com/

And our experts will gladly present our various expertise or present optimised solutions to your requirements.

itl

Intercontinental Trust Ltd