A QUICK GUIDE TO TODAY'S CYBER THREATS

Introduction

Understanding the cybersecurity landscape

In this booklet, we will be showing you some of the techniques that are being used by cybercriminals intent on taking advantage of the human element of the IT chain. There is some excellent technology being deployed in businesses and homes now, and so many cybercriminals are targeting the perceived weakest link, us. We will try to illuminate you as to how you can spot an attempt to manipulate you into presenting the
criminal with the opportunities they require to bypass the technology that we use to keep IT safe.

So why target humans? Simply put, a human being can override the security by either passing information freely, or by running some software or code from the ‘safe’ side of the IT network. In essence, the cybercriminal is asking you to open the door and let them in. The best defence is to be vigilant of these attempts, just as you would do at home or even in the office if a stranger attempts to gain entry.

We will describe to you how the attempts are made, and how you should deal with them. Above all the real message is to stay safe, and we hope this booklet will help you to do just that.

In this book

- Social Engineering
  - Phishing
  - Spear Phishing
  - Phone (or Voice) Phishing
  - Email from a friend
  - Malvertising
- Cyber Security Best Practices
  - Safe browsing
  - How to spot bad attachments
  - Good password practice
  - Email from a friend
- Security Tips

SOCIAL ENGINEERING

When the term ‘Social Engineering’ is used in the context of cybersecurity, or cybercrime it is a generic term for any attempt to have an end user assist the perpetrator by having them do something. Outside of the cyber realm this would be better known as conning (confidence trick) or scamming somebody.

Phishing

Via email mainly, this describes when an email is received that resembles an authentic email sometimes (but not necessarily) even from a genuine
sender.

These emails are trying to illicit a response that will in turn provide some information to the originator.

A common example of this is when you receive an e-mail from your bank, with what seems to be a legitimate return address, requesting you to perform a task such as confirming your banking password or personal details.

PHONE (OR VOICE) PHISHING

This type of social engineering is becoming popular as it adds a level of human manipulation into the attack.

The scam artist will initiate a call to randomly pre-selected numbers and then proceed to try to gain information or access to machines. Sometimes also known as pretexting, the scammer uses techniques to convince the called party that they are a genuine caller requiring some information or access to assist with an action. The caller will establish
a rapport, and using known large organisations for cover (think Microsoft, Apple or BT) and with a little probing will trick called parties into confirming or correcting information over the phone.

In some recent cases presented to Urban Network, we have heard of callers requesting that members of the public divulge personal information to callers as part of a greater scam. In other cases, the caller suggests that they are working for a reputable software vendor like Microsoft and need assistance gaining access to the user's PC to 'verify a known threat'. Of course, no genuine caller would ask for personal information, or to get access to a machine that was not instigated in the first instance by the called party.

Malvertising

What is Malvertising?
This is a combination that describes the cybercrime of using advertising on websites to proliferate malware. This is now one of the most successful ways that cybercriminals have of spreading bad code, or malware and infecting machines.

How does it work?
Malvertising is when a cybercrime ring using legitimate sites, use the adverts that automatically populate when you visit a page. A user could be simply checking the news on a well-known, and reputable site and when you 'land' the page automatically begins to load a myriad of additional pages in the form of adverts in thumbnails.
These are provided by ad networks, and the legitimate owners are not aware of the locations they go to, as they are not hosted by the owners. Instead, the pages are hosted by the networks and are quickly swapped out with new ads all the time.

As this is the case, cybercriminals are purchasing ad space, usually anonymously by using stealth methods to hide their identity, and get their malware appearing all over the web. This is particularly aided by adding intelligence from the ad networks, and allowing targeted attack profiling by examining the search criteria of the searching party from their browsers. For example, if a criminal was targeting a shopper who was using an old browser, they may look for searches with 'shopping' 'buying' etc. and then throw up a bad site if the browser is an old revision with known exploits.

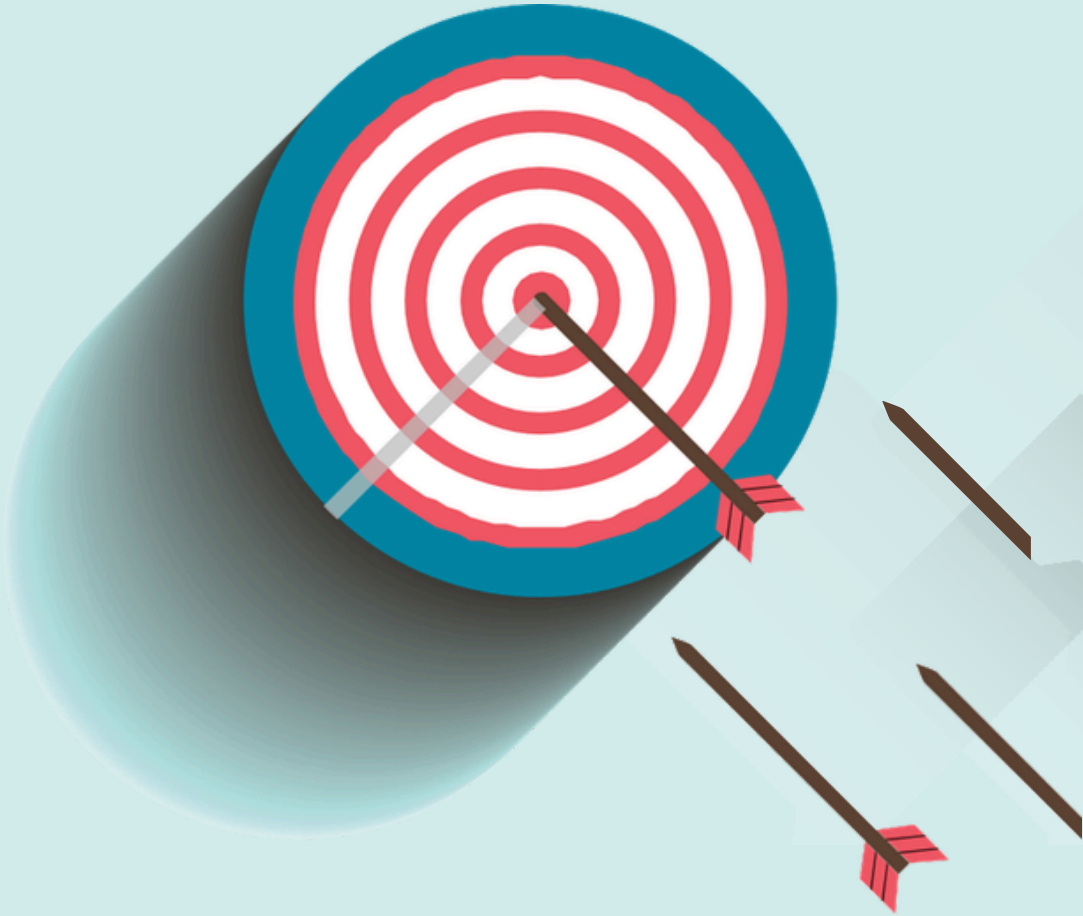
As this method actually costs the attackers time and money, it is safe to assume that it is very lucrative for the cybercriminals. After all, they are efficient and productive, so this technique must be rewarding for them. Finding the criminals after the fact is difficult due to the nature of the ad networks dealing with so many adverts, and the relative ease of obscuring identity on the web.

Spear Phishing

Spear Phishing may be defined as ‘highly targeted phishing aimed at specific individuals or groups within an organisation’.

Due to the amount of information that can be found freely with just a little digging around online from sites like LinkedIn, Facebook and company’s own websites it is possible to add convincing details to Phishing scams. Spear Phishing emails, for instance, may refer to their targets by their specific name, rank, or position instead of using generic titles as in broader phishing campaigns.

This type of scam is now becoming much more abundant, a 2016 Verizon Data Breach Report* states that over 80% of malware infestations are delivered in this targeted way.



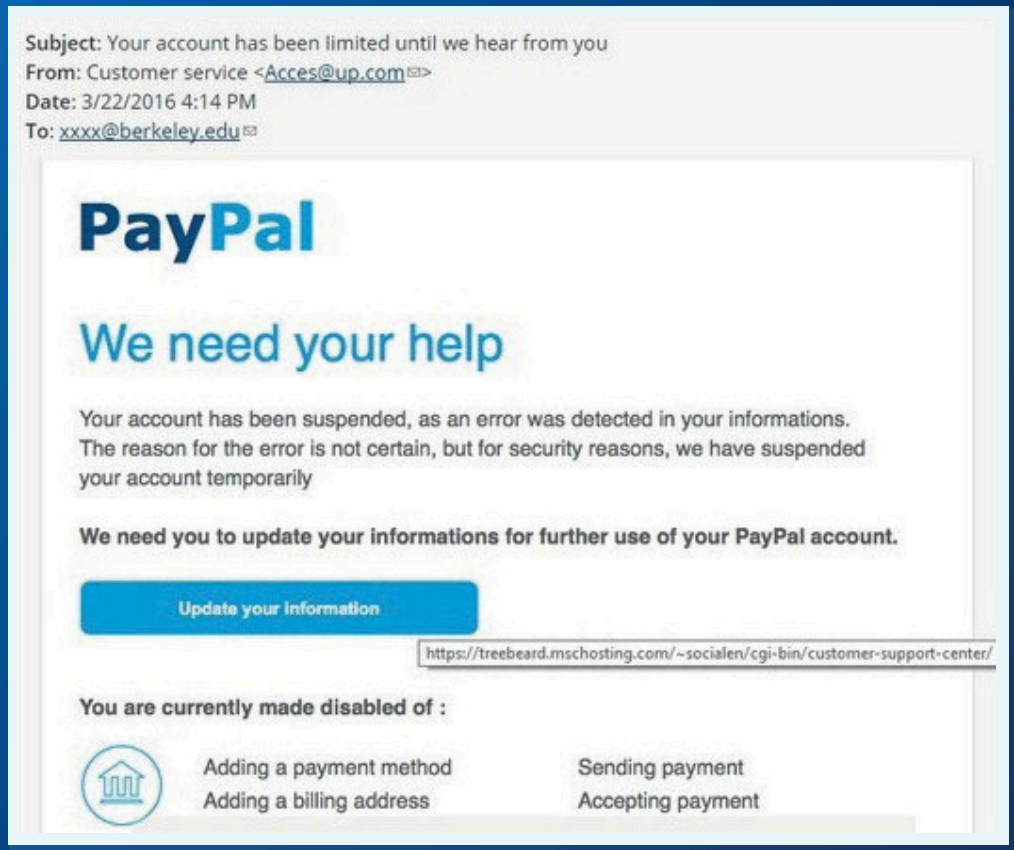
How To Spot A Fake Email

The message contains a mismatched URL
Check the integrity of any embedded URLs. Often the URL in a phishing message will appear to be perfectly valid. However, if you hover your mouse over the top of the URL, you should see the actual hyperlinked address (at least in Outlook). If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent or malicious.

The message asks for personal information
No matter how official an email message might look, it's always a bad sign if the message asks for personal information. Your bank doesn't need you to send it your account number. It already knows what that is. Similarly, a reputable company should never send an email asking for your password, credit card number, or the answer to a security question.

You didn't initiate the action
If you received an email message informing that you have won a contest you did not enter or won the lottery but you never bought a lottery ticket, you can bet that the message is a scam.

The offer seems too good to be true
There is an old saying that if something seems too good to be true, it probably is. That holds especially true for email messages. If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.



CYBER SECURITY BEST PRACTICES

SAFE BROWSING

The World Wide Web is a wonderful thing, never has it been so easy to find information, research your favourite topics or shop from the comfort of your armchair; it's brilliant.

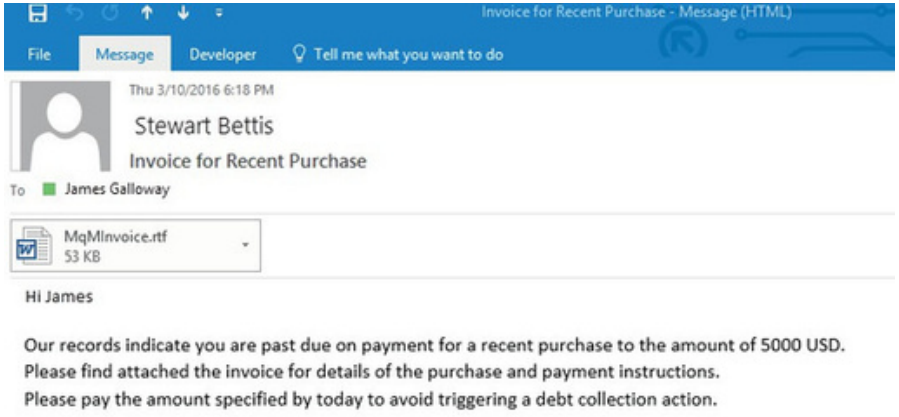
But it is also a haven for bad software, viruses and spyware (Spyware is software that tracks your browsing and PC activity and sends the information to 3rd parties) that can infect your devices if you are not careful.

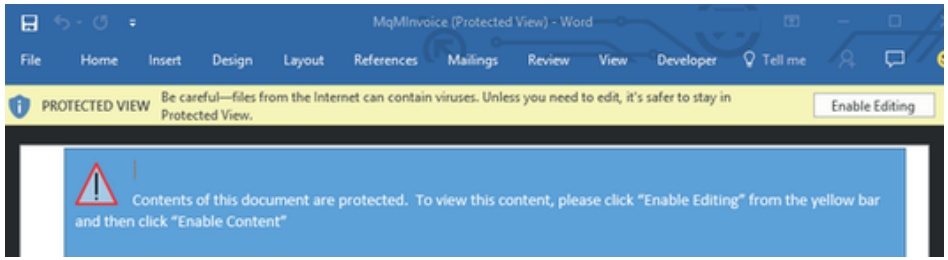
How To Spot Bad Attachments

In 2015, we observed an increase of macro-based malware along with the spike in spam volume. The majority of the macro-based attacks often start with spammed messages containing attachments such as Microsoft Word document and Excel files. These messages often use attention-grabbing topics, mostly related to finances, such as remittance and invoices for services. Macro malware, as we have seen throughout the past year or so, is experiencing a revival of sorts. Thought to have been banished in the early 2000s, macro malware is proving to everyone that old threats die hard.

What are macros?

Macros are a set of commands or code that are meant to help automate certain tasks, but recently the bad guys have yet again been utilising this heavily to automate their malware-related tasks as well.





Good Password Practice

DO

- Create unique passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters.
- Password complexity is good, but the length is key. Increasing password length to 12 characters can increase password security significantly. Tips: turn a sentence into a password, also called a ‘pass phrase’. For example, the sentence ‘This is my password & it’s for my eyes only!’ is easier to remember than ‘Syz8#K3!’ and far more secure.
- Passwords need to be changed on a regular basis: every 60 days is OK, but every 30 is better.

DON'T

- Include your personal information (name, birthday) or username in your password
- Use easily guessed passwords i.e. ‘password’, keyboard patterns such as ‘123456’, ‘qwerty’ or words in the dictionary.
- Avoid using the same password for multiple accounts.; one hack exposes many accounts.

Email From A Friend

In some cases, cybercriminals may have managed to gain access to systems belonging to somebody that you know and trust or potentially they have spoofed their address (sending with the correct email address but not actually gaining control of the person's accounts).

This could be email, but just as likely it could be their social media accounts or any online system really. Using genuine accounts, the cybercriminal masquerading as your 'friend' may send you a link, or attachment extolling that you 'must see this amazing...' or some other hook.

These attempts are very hard to spot, and it would be difficult to tell on the face of it whether the contact is genuine.

Security tips

Following some simple guidelines can prevent the exposure to these risks:

- Keep your browser up-to-date with the latest patches.
- Uninstall plug-ins you don’t need to secure your web browser and ensure plug-ins you use are updated regularly and automatically.
- Install good protective software like Anti-Virus and Anti-Spyware and good hardware such as Firewalls it is possible to minimise infection.

Read more about some best free Anti-Virus & Anti-Malware the Urban Network tech guys have picked up for you at urbannetwork.co.uk/blog

Security tips

- Verify the request. Make a call to the genuine sender, ask if they have sent you an email and what it was.
- Question all email requests. Avoid responding to the request, do not give any information in reply.
- Have protocols for accounts teams to follow before issuing payments

Security tips

If you receive a call asking you to give information or access, it is almost certainly a social engineering attempt to trick you. Hang up, if you feel the need call the organisation yourself using a known genuine number (e.g., a bank number on the back of your card) and ask if you have been contacted.

Be wary of any inbound call where the caller is asking for your personal information, this is simply not how it works, and even if on the rare off-chance it is, then calling them back is perfectly acceptable.

Security tips

- Where you receive an email that appears to be from someone you know, consider if the communication sounds right. E.g. Does your brother usually send you dramatic emails or cat videos? If not it’s unlikely he just started so ask him or just delete it, it can always be resent.

- Hover your mouse over a sender’s name in the ‘from’ field or touch it on a tablet, it will produce the full reply address which should be correct. If it isn’t it is likely a spoofed email. Delete it

- Does the general body of the message feel right, if anything doesn’t read OK to you, pick up the phone and ask the sender (as you know them in this case) if it’s genuine. Checking is safer than being caught out.

Security tips

- Make sure your browsers, plug-ins, and operating systems are kept up-to-date.
- Malvertising is simply a vehicle for finding security flaws hiding elsewhere in your system.
- The simplest way to minimise these problems is to tighten up vulnerabilities on your computer.
- Uninstall browser plug-ins you don’t use and set the rest to click-to-play. Click-to-play plug-ins keep Flash or Java from running unless you specifically tell them to (by clicking on the ad). A good bulk of malvertising relies on exploiting these plug-ins, so enabling this feature in your browser settings will offer excellent protection.

Signs to watch for

- Take notice of the reply address, does it look real, is the syntax correct? Often the reply address can show if the sending party are who they are representing themselves as.
- If you're asked to follow a link, and it seems authentic then there should be security on the site if you are entering personal details. Look for the secure S after the http in the URL (https://) so you know that the site is secure. It is unlikely a cybercriminal will secure the sites they have put up which require additional time money and administration.
- Double check any links that are in the body of emails. If you hover your mouse over (or long press on a smart device) a link is displayed. If it doesn't start with the correct address, then chances are it's a scam. Don't click links without checking them first.
- Check the overall grammar or spelling of the email. In many cases, the format is not quite right or the request seems a little unprofessional. Cybercriminals don't normally have a proofreading stage, and you can see this a lot of times in the quality of their communication.

Security tips

If you receive an email that flags up with any of the above signs, simply delete it permanently. Clicking links or following the advice can potentially infect your machine, and replying with any information will compromise your identity for theft. If something just doesn't feel right, delete. Genuine requestors will follow up with their other contact details, or you can verify with them yourself if you need reassurance.

What happens when the user opens an attachment and enables macros?

Most documents that carry macro-based ransomware include some sort of explanation or excuse to encourage you to ‘enable editing’ and change your security settings – often, ironically, under the guise of improving security somehow.

Enabling macros in this instance will have the allow the PC to run the code and download the Ransomware as an EXE (Windows program) file and run it.

The most likely outcome for this type of threat is that the malware will attempt to encrypt all data it can access. This type of malware is termed as Ransomware, and will attempt to encrypt all data the PC or users have access to and render it useless. It will then typically change the user’s desktop with a ransom notice requesting payment to receive the key enabling you to unencrypt your data.

Security tips

- Ensure your accounts don’t all have admin rights or access to data they don’t need to always have.
- Disable Macros wherever possible
- Implement a robust patching/update cycles on all IT hardware
- If you have mail filters, have it block dangerous file types (e.g., zip files)
- Consider disabling USB ports unless they are essential
- Backup, image based are the best type, but files if nothing else

CYBER SECURITY IS EVERYONE'S BUSINESS

Cybercrime could happen to anyone.

It is important to understand current trends in security threats, be able to identify vulnerabilities, and protect your data against these threats.

urban.

Coppergate House,
10 White’s Row, London, E1 7NF

0333 188 9155| urbannetwork.co.uk