East Midlands Special Operations Unit

CYBER AND FRAUD PROTECT WEEKLY SECURITY ARTICLE

Thursday 14 January 2021

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands to raise awareness among businesses and the public.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team

Social Engineering: How I might attack your organisation

It's quite common to hear about cyberattacks causing huge data breaches and resulting in businesses suffering irreparable harm. Such articles encourage us to imagine sophisticated hackers in cyberspace, employing state of the art technologies to infiltrate your computer systems.

For many clinics, the answer always seems to lie with either:

- Investing heavily in new technologies to bolster network defences
- The ostrich effect - stick your head in the sand and hope the problem goes away.

Alternatively, you can let apathy sink in - not much you can do about it, right? Problem is, you've already made your biggest mistake – what makes you think I'm going to target your IT systems? That's the goal, not the attack vector.

If I want to hit you with ransomware, steal patient confidential data or just fool you into handing over some of your over stretched budget, I'm going to target **you**. You are the weakest link in the chain.

Indeed, if you study credible public reports and expert analysis on cybersecurity incidents, you'll discover that approximately seven out of ten incidents occur due to human error and behaviour, not complicated technical attacks. As such, cyber security, is fundamentally a human issue, not a technology one. If you want a cheap, effective solution to cybercrime – train your staff.

Example one: Vishing

Someone will call and trick you into divulging sensitive information.

They do this by using one or more of these techniques:

- **The authority principle**: They will claim an important job title to convince you to hand over data.
- **The intimidation principle:** They will act belligerently, telling you that there will be unpleasant financial or legal consequences. This prevents the target from thinking straight.
- **The familiarity principle:** Conversely, they may be very personable or seek common ground to create a bond between you and them.
- **The trust principle:** Involves citing professional credentials or known organisation information to sound credible.
- **The social proof principle:** They may claim that you both know a trusted third party which implicitly suggests that they are also trustworthy - we all know each other!
- **The urgency principle:** Finally, the social engineer might claim that a situation is urgent or that he or she has very little time to verify their identity.

Example two: Phishing

It's not just fake calls that are hitting organisations. Phishing emails are also a big concern.
If I was a cybercriminal, I would spend considerable time and effort researching your organisation and suppliers in order to craft emails that appear to be legitimate. At that point, all sorts of problems might ensue. For example

- **Steal credentials:** I could include a link. If you click the link you'll get sent to a bogus website that looks like East Midlands LTD. If you type in your credentials, I'll capture them and have unrestrained access to your online account.
- **Infect your machine:**
  + Alternatively, you might click the link and get taken to my site. My web page will automatically scan your computer for a security weakness – quite often, people fail to shut down and restart their machines, meaning security patches have not taken effect. If your machine is vulnerable, I'll download a Trojan that lets me take over your system. At that point, I can sit on your network for months quietly exfiltrating data. Alternatively, I'll just deploy some ransomware and be done with it.
  + Finally, I might include an infected attachment. Macro documents, for example, can often contain viruses that aren't picked up by antivirus software – especially if that software is a little out of date.

Mitigation – Protect yourself and your customers

Remember: **You** are the data owner. GDPR says **you** must look after it. Failure to give your staff basic cyber security messages suggests negligence or incompetence. Tell them to:

Vishing:

- **Keep abreast of the news.** As awful as it may seem, knowledge of attack methods and techniques will hone the ability to separate fact from fiction.
- **Understand** that a legitimate organisation won't make unsolicited requests for sensitive information. Anyone who does this over the phone is probably trying to scam you.
- **Call back using official channels.** No matter how friendly or stressful the call might seem, ask yourself, 'how can I contact the company or an official representative through official, well known channels?' Once you know the correct communication channels, verify the claims being made.
- **Don't give into pressure**. If someone tries to coerce you into giving them sensitive information, hang up.

Emails:

- **For high value operations**: Always check the 'from' field carefully. Look for variations in spelling, amendments and simple transposition errors (e.g. BBC.com not BCB.com). Hovering your mouse over a link will also identify where it actually goes rather than where it claims to go.
- **Look for a break in protocol.** If the email deviates from normal procedure, such as a request for payment - seek confirmation from official channels.
- **Test Employees:** Use an open source phishing tool to train and then test staff's ability to detect and report phishing emails. You can easily search for one using your favourite search engine.
- **Guard sensitive data.** Encourage all employees to research their name online. A social engineer will use this information to hack you, so:

- **Remove your data from websites** by using the **'contact us'** part of any web page. Under GDPR, everyone has the right to 'be forgotten' and can request the removal of their personal information. All companies must comply with this.
- **Review your privacy settings** for online social media accounts. Remember, if I can't find information on you, I'll scope your friends and family, so advise them to do the same.

Ideally, you need to train staff to recognise what sensitive data is and the impact it will have on the organisation if this information was exposed. Knowing why information is sensitive will encourage others to take better care of it.

Warning

Using social engineering to commit fraud is a crime.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).