Awareness raising campaign for SMEs

Guidance for Organisations on Phishing and Social Engineering Attacks

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

One of the main obligations under the General Data Protection Regulation (GDPR) for organisations which process personal data ('controllers'), is that they must do so in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing (including theft, destruction or damage, or disclosure) using 'appropriate technical or organisational measures'. This is sometimes referred to as the principle of 'integrity and confidentiality' or the 'security principle'.

This obligation is an important one, which controllers should be cognisant of, particularly those who utilise or store sensitive personal data. Whether or not an organisation has appropriate technical and organisational measures in place to ensure the security of the personal data they process is one of the first questions the Data Protection Commission (DPC) is likely to ask in the event of a personal data breach or the exercise of the DPC's investigative powers. Controllers can also consult the DPC's guidance for controllers on data security when assessing the appropriate security measures they need to implement.

One way in which the risks regarding security of personal data can arise is through what are known as 'phishing' or 'social engineering' attacks. Phishing is an example of a type of social engineering which is commonly used to deceive users. Phishing is where someone fraudulently attempt to trick users into disclosing sensitive information, such as usernames, passwords, or credit card details, by disguising themselves as a trusted source in an electronic communication. By using a trusted source, or name, or familiar logo as 'bait', attackers can go 'fishing' for sensitive information, such as personal data.

This can be done in many ways, such as 'email spoofing' (where cloned or similar looking email addresses or names are used) and misdirecting users to enter sensitive information into a fake website (which looks very much like the legitimate one), or download harmless looking but malicious software (often disguised as email attachments).

Tips to Spot Phishing or Social Engineering

Email Spoofing: Email spoofing involves an attacker sending messages with a forged sender address. Because the core technical protocols for email don't have a mechanism for authentication, attackers often use spoofing to mislead the recipient about the origin of a message. Systems such as SSL/TLS for email encryption may help avoid this risk, however are often not available or utilised for this purpose in many organisations.

- ✓ Most email providers do provide some security measures to protect against these sorts of emails, but it is important to double check senders' details, particularly if an email is otherwise suspicious.
- ✓ For example, ensure both the email address itself, as well as any contact name or name in the body of the email matches up.

Spear Phishing: Spear phishing is a targeted form of phishing, where the attacker seeks to make their attack seem more legitimate by tailoring it for the intended victim. This is common for more senior members of an organisation, or staff who have responsibility in a sensitive area. The attacker might have done their homework and included the correct name, job title, email address, etc. of the intended victim.

- ✓ It is particularly important for organisations to make their staff who work in such areas aware of the risk of targeted phishing attacks, and ensure that they are wary of any electronic correspondence which they are not expecting.

Link Manipulation: Phishing often involves a technical deception designed to make a link in an electronic communication look like it belongs to a trusted source. Phishers may use misspelled URLs or legitimate-sounding subdomains to trick users into clicking a link. For example, the URL 'www.truztedsource.ie' might be used to trick users into clicking a link they think is for 'www.trustedsource.ie'. Likewise phishers might use a link like 'www.trustedsource.secureinfo.ie' to trick users into thinking it links to a 'secure info' page on the 'trustedsource' website, but it would actually link to the 'secureinfo.ie' website, which could be a fake page set up by the phisher. Sometimes the displayed text for a link looks like a legitimate URL, but the link when you click it leads somewhere else – for example, http://www.trustedsource.ie/ actually leads to 'ww.notatrustedsource.ie'. You can often see where the real link leads by hovering your cursor over the link, but it is important to remember that this is not always possible, such as in the case of most mobile applications.

- ✓ Organisations need to ensure staff are wary of clicking links to external websites, particularly on mobile devices.
- ✓ Organisations should consider implementation of technical security measures which can help to detect and protect against link manipulation.

Social Engineering: Social engineering can take many forms and normally uses subtle psychological techniques to trick users into taking a certain action. Users might be encouraged to click on various kinds of unexpected content, such as links or attachments, for various professional, technical, or social reasons. An email might come into a work inbox marked 'Important!' or 'URGENT', with a title and wording that seeks to trick staff into quickly opening an attachment or clicking a link. A fake security popup may seek to scare a user into clicking a link by telling them that they have been infected with malware, or need to update their security software. Or an ad or email may simply encourage someone to click a link by pretending to link to some very interesting workplace gossip, or an outrageous news headline.

- ✓ Organisations can remind staff about the danger of reacting to electronic communications even where it appears urgent.
- ✓ Organisations should consider organisational or technical measures regarding which links can be clicked or attachments downloaded by staff, where appropriate.

Phishing and other social engineering practices can be very convincing and present a real risk for organisations, particularly workplaces with many staff and/or a high volume of electronic communications. It is important that, as part of their overall data security policies, organisations consider if they are vulnerable to such attacks, and what 'appropriate technical or organisational measures' they can take to reduce any vulnerabilities.

Approaches to mitigating the risk of attacks

Organisations can take many steps to protect themselves from data security risks such as phishing and social engineering, such as: conducting regular and detailed risk analyses; reviewing internal communications and IT policies; and implementing physical and technical security measures and staff training.

Organisations should consider the state of the art in technical and organisational measures, and the costs and proportionality of implementing certain measures – the decision should take into account not only the best and most appropriate applicable technology, but also both the size and nature of the organisation, as well as the volume and nature of the personal data stored and otherwise processed.

Organisations also have to take into account obligations regarding ensuring the security and integrity of any data processing which is done of their behalf by data processors, including whether the data processing agreements sufficiently cover the requirements around security and integrity of processing and what to do in the case of a security incident or personal data breach.

Certain services utilised by organisations, such as cloud-based email services, may offer many advantages to organisations. However, they can also introduce technical security vulnerabilities, which organisations need to recognise. Failure to implement appropriate compliance and security controls can increase the risk of a personal data breach from phishing or social engineering attacks. Organisations need to implement countermeasures to protect against threats both generally, and specifically introduced by the software and services utilised by the organisation, such as - unauthorised access to personal data, hijacking of accounts, identity theft, cyber fraud, and hacking.

Cloud-based 'groupware' (software that helps groups of colleagues collaborate and organise their activities), for email and other professional functions, such as Microsoft's Office 365 and Google's G Suite provide advanced settings and solutions, which can assist organisations in securing and combating these threats. Email providers, in most cases, also provide best practice guidance to assist organisations in securing its email service.

Alongside appropriate technical security measures, staff training is obviously one of the best ways an organisation can reduce its vulnerability to phishing or social engineering. Training can – alongside appropriate technical security measures – by ensuring that staff, particularly those staff working with sensitive information such as personal data, both understand the risks and are equipped to avoid risks, such as by not opening emails from senders they are not familiar with, and avoiding clicking links contained in an email unless you they exactly where it is going.

A layered approach to security mitigates the risk of a single security measure failing which can result in a breach of personal data by an organisation.

Recommendations to increase security against attacks

The following recommendations may assist organisations when considering which technical and organisational measures need to be implemented to ensure the security and integrity of the personal data which they process and protect against phishing and social engineering attacks. Not all recommendations will be relevant to every organisation, but they should be considered in the context of the work of an organisation and the types of data processing it engages in, to implement those most suited in each case:

- ✓ Review any default security settings, including passwords and credentials, provided by any email service or groupware utilised by the organisation.
- ✓ Apply multi-factor authentication for administrators, web-based or remote users of email, databases, or organisation systems, including any managed service partner or administrators.
- ✓ Implement rules to filter and detect suspicious and/or spam emails.
- ✓ Create rules for how messages and attachments are handled based on conditions such as file type or message size.
- ✓ Turn on auditing to ensure there is an audit log available to track user action on the email system.
- ✓ Ensure users have the correct role-based email permissions - with regard to system rights, management or configuration.
- ✓ Disable remote or web-based access to email, databases, or other systems, for staff that are primarily office-bound.
- ✓ Implement controls to prevent users automatically forwarding email(s) to external email addresses.
- ✓ Regularly review any forwarding rules enabled for email-based groupware to ensure there is no unnecessary or unapproved rules.
- ✓ Configure a policy to provide a warning (visual cue) when an email is sent to an external contact or organisation, (e.g. Office 365 Safety tips).
- ✓ Configure policies to provide alerts about sign-in behaviour such as irregular geolocation access.
- ✓ Configure a data loss prevention policy to automatically identify and monitor any sensitive information (e.g. bank details) being emailed to external addresses.
- ✓ Regularly review web access policies (filtering) to prohibit access to malicious (phishing) or inappropriate web sites.
- ✓ Implementing a control process for approving and securing all devices that access email.
- ✓ Create appropriate email access policies for areas such as a Bring Your Own Device (BYOD).
- ✓ Manage mobile devices by enrolling them in a mobile device management solution (to potentially locate, lock, and wipe if lost).
- ✓ Keep and regularly review an inventory of mobile devices approved to access email and remove any devices that are no longer required.
- ✓ Develop an incident response plan to provide a framework for the management of any security incident(s).
- ✓ Require that emails are transmitted via a secure (encrypted) connection such as TLS 1.2.

- ✓ Review any email archiving policies to reduce the volume of information contained within mailboxes.
- ✓ Implement encryption at rest for mailboxes.
- ✓ Issue relevant updates to staff on the importance of remaining vigilant of attempts at social engineering via email and other attack vectors. Integrate these updates into a continuous education process about cyber security and associated threats.
- ✓ Ensure staff are able to contact someone, such as a manager, or internal or external IT expert, where they have concerns about data security risks, such as a suspicious communication, link, attachment, or popup.
- ✓ Consider implementing advanced email protection methods such as Sender Policy Framenwork (SPF), DomainKeys Identified Mail (DKIM), Domain Based Message Authentication, Reporting and Conformance (DMARC).

Organisations are reminded that under the GDPR organisations must report personal data breaches to the relevant supervisory authority where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay. Further guidance on breach notifications can be found on the DPC's website.