Security Best Practices

July 2018

AlasConnect

Social Media Safety

- Treat social media as a public forum. Once you put it online, you have no real control over who sees it.
- Use strong privacy and security settings provided on social media sites
- Do not use the same password on your Internet accounts as you do on your corporate accounts or local PC
- Only share and connect with people you know
- Don’t click on ads or participate in surveys
- Avoid suspicious third party apps and games
- Don’t access personal social media sites from a business PC

Social Media Safety

- Example

If an attacker wants to target their attack, they may look at your social media accounts (e.g. LinkedIn and Facebook) to see who you work with and what your job duties and access levels are. Using this information they will craft an attack to try and trick you.

A common example is targeting the CFO or Controller of a business with requests appearing to come from legitimate sources (fake invoices, fake wire requests) in order to trick them into issuing payments. Many businesses have fallen prey to this sort of confidence game.

Avoiding “Phishing” and Scams

- Always be suspicious of email, if in doubt you should talk with someone over the phone or meet them in person (even inside the organization) to defeat spoofing
- Always verify the sender is someone you actually know
- Be on the lookout for unusual behavior or strange “speech patterns”
- Never authorize important transactions based solely on email authorization
- Never open an unsolicited attachment
- Never click an unsolicited link
- Never respond to spam email messages
- Never send passwords, account names, confidential data or bank information by email
- If your web browser shows a security warning, close the page

Avoiding “Phishing” and Scams

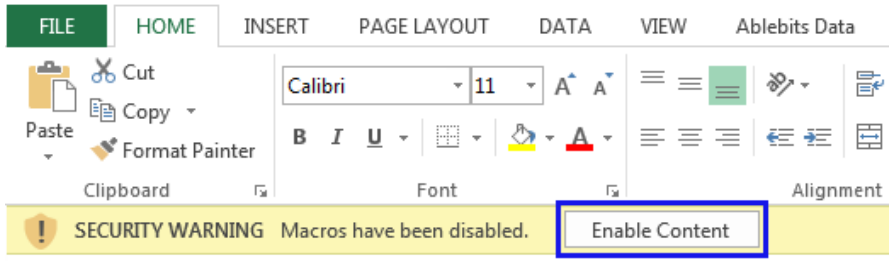
- Example:

Many times attackers will use “social engineering” to attempt to gain your trust by spoofing emails from a co-worker inside the organization. They may ask you to open a PDF document, look at a funny video or send them a password. This can compromise your security and provide an avenue for attack!

Commonly scammers will use a similar domain to spoof an email. For instance, the “.co” domain is very similar to “.com”.

Documents with “Macros”

- Microsoft Word and Microsoft Excel documents can include embedded “macros” which are a vector for malware
- Don’t click on “enable macros”, especially if you don’t know exactly where a document came from



Passwords

- Use longer, complex passwords and change your password often if possible
- If you have the option to use Two Factor Authentication (2FA) enable this feature
- Try to avoid using dictionary words
- Use different passwords for different accounts that you use
- Don’t re-use an old password; completely change the password to something else
- Never share your account with anyone
- Avoid “remember my password” options when logging into different websites, especially on shared computers

Passwords are a pain!

- Everyone has too many passwords and it is almost impossible to remember them all
- Don’t write down passwords or store them in a text file, use an encrypted password safe instead (KeePass is a free one)
- Use a single password to secure your password safe, and put all your other passwords in the safe for easy access
- Never share access to your password safe
- Secure your password safe with 2FA

Good Security “Hygiene”

- Never use illegal or “cracked” copies of software
- Be careful which wireless networks you connect to and only use trusted networks
- Password or passcode protect your mobile device (tablet/phone)
- Lock your workstation when you walk away
- Keep printed confidential information out of sight (clean desk) or in a locked cabinet
- Only connect to the Internet from behind a trusted firewall