ADVISOR SOLUTIONS GROUP, INC

INTEROFFICE MEMORANDUM

TO: [RECIPIENT NAME]
FROM: [YOUR NAME]
SUBJECT: HACKING AND MALWARE
DATE: [CLICK TO SELECT DATE]
CC: [NAME]

Information Security

Information Security is an important priority at any company. This memo will address how to protect against hacking and malware.

Phishing

Protect against phishing which is a technique used by online criminals to trick people into revealing information. Most are fairly easy to recognize as scams but some can emulate notifications from well-known vendors such as UPS, Federal Express, Amazon or Ebay. Examine emails carefully, especially the sender's email address. If the email domain does not match the sender's company it is likely fake. Also examine any links by hovering your mouse over the link to see the linked address. This is not 100% reliable so the best policy is to not click on any links. Instead, open your browser and enter the address manually.

Spearphishing which is also known as pretexting or social engineering is more insidious. Spearphishing attacks are targeted and the criminal will often glean information from social media sites including names of family or friends to tailor the phishing attack. These can be much more difficult to detect so be careful.

Scareware

A common ploy is fake antivirus security warnings also called scareware. Everyone on the [COMPANY] network has antivirus software but you should also know what type of antivirus software is protecting your other computers. If a warning pops up react calmly and with caution.

Malware

Malware is malicious software that can be loaded via the internet, downloads, attachments, email, social media and other platforms. The most damaging variant of malware are keyloggers which log every keystroke enabling the hacker to obtain usernames and passwords typed on the computer. The best defense against malware is a combination of current antivirus software, up-to-date systems, proper browser security settings and user awareness. Every browser should restrict cookies to some degree and block pop-ups. A security setting of "medium" or higher should be used.

Flash Drives

Many flash drives contain pre-installed viruses. Be aware of the source of a flash drive and do not use a drive from an unknown or untrustworthy source. When using a new flash drive for the first time, hold down the left Shift key when inserting the drive to block viruses or malware from auto-executing.

Prepare and Be Aware

The key to strong information security is to prepare and be aware. Be sure to report any incidents or suspicions. Please contact [BLANK] if you have any questions or concerns regarding information security.