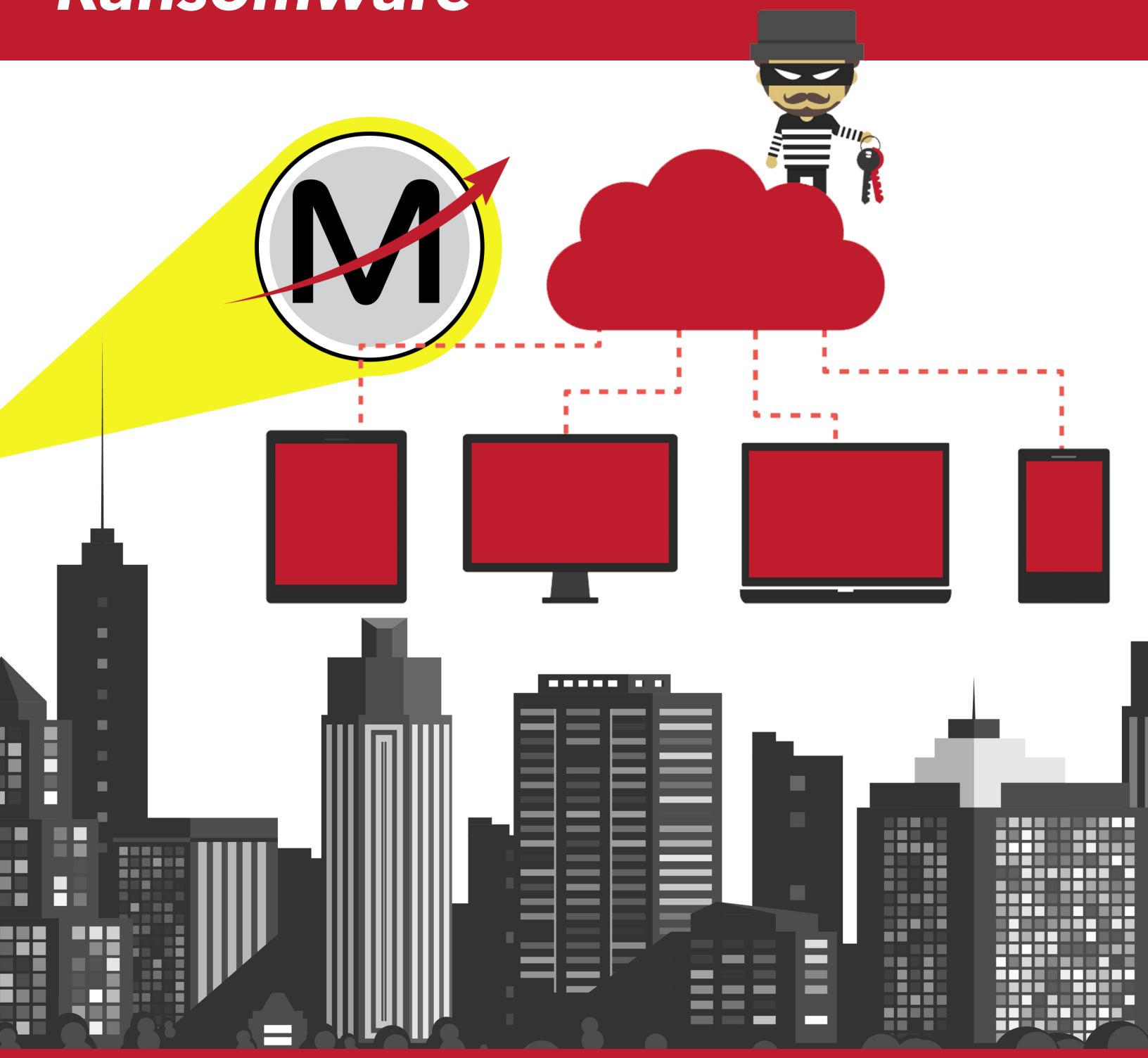
TIPS TO SPOT Ransomware

in Your Email Beforehand



MAXtech

614-401-8800

www.maxtechagency.com

RANSOMWARE IS A FORM OF MALWARE

Ransomware is a form of malware that blocks or limits access to your ***and/or files and then demands a ransom be paid to the scammer for***

Cybercriminals may pretend to be from the police or a federal law enforcement agency (think F.B.I or C.I.A.) and display a message on your infected computer claiming you have been involved in illegal activity and must pay a fine, or they might simply demand payment for a 'key' to unlock your computer. They might even give you a deadline to pay ransom or risk having your files permanently deleted or destroyed. Even if you pay the ransom, there is no guarantee your computer and/or files will be unlocked.

As you can see, ransomware is the last thing anyone wants to be dealing with on their computer. But ransomware attacks happen all the time, and they often occur via email. So it's important to be aware of the telltale signs of a ransomware email (and, ultimately, other malware emails) beforehand to avoid computer infections and inaccessible or lost information. If you see any of the signs below, don't click anything in the email and don't forward the email to anyone (with one exception, discussed later in this article). Simply delete the email.

Weird "From" Addresses – Sometimes it's obvious you're receiving ransomware emails because some of the email addresses they're coming from are entirely nonsensical. But wannabe attackers can easily create fake email addresses that are almost identical to other major companies' email addresses. Customerhelp@amaz0n.com could easily be misread as an official company email address. Even savvier cybercriminals can spoof official email addresses so that any emails they send look and seem legitimate. So always double check the email's content by typing the business' official URL into another tab or browser window and manually logging in to your account to see if your account information or messages match the information in the email.

Odd Emails – If you've received an email you're not expecting and it seems unusual or isn't relevant to you directly, chances are it's a typical phishing email, even if it looks like the sender is from within your organization. If in doubt about who the sender is, call or message the "sender" (message via text or an online chat service, NOT email) to confirm its legitimacy.

Dear Friend – If you've been addressed in the subject line and/or email content with a generic salutation and not by your name, the sender more than likely doesn't know who you are. At best, it's just a spam marketing email, but at worst, you're a target of a cyber-criminal who wants access to your personal information.

Badd gramar/speling – Most peopl take a since of pride in there work. badd gramar, typos and speling is a dead givway that they're is something phishy.

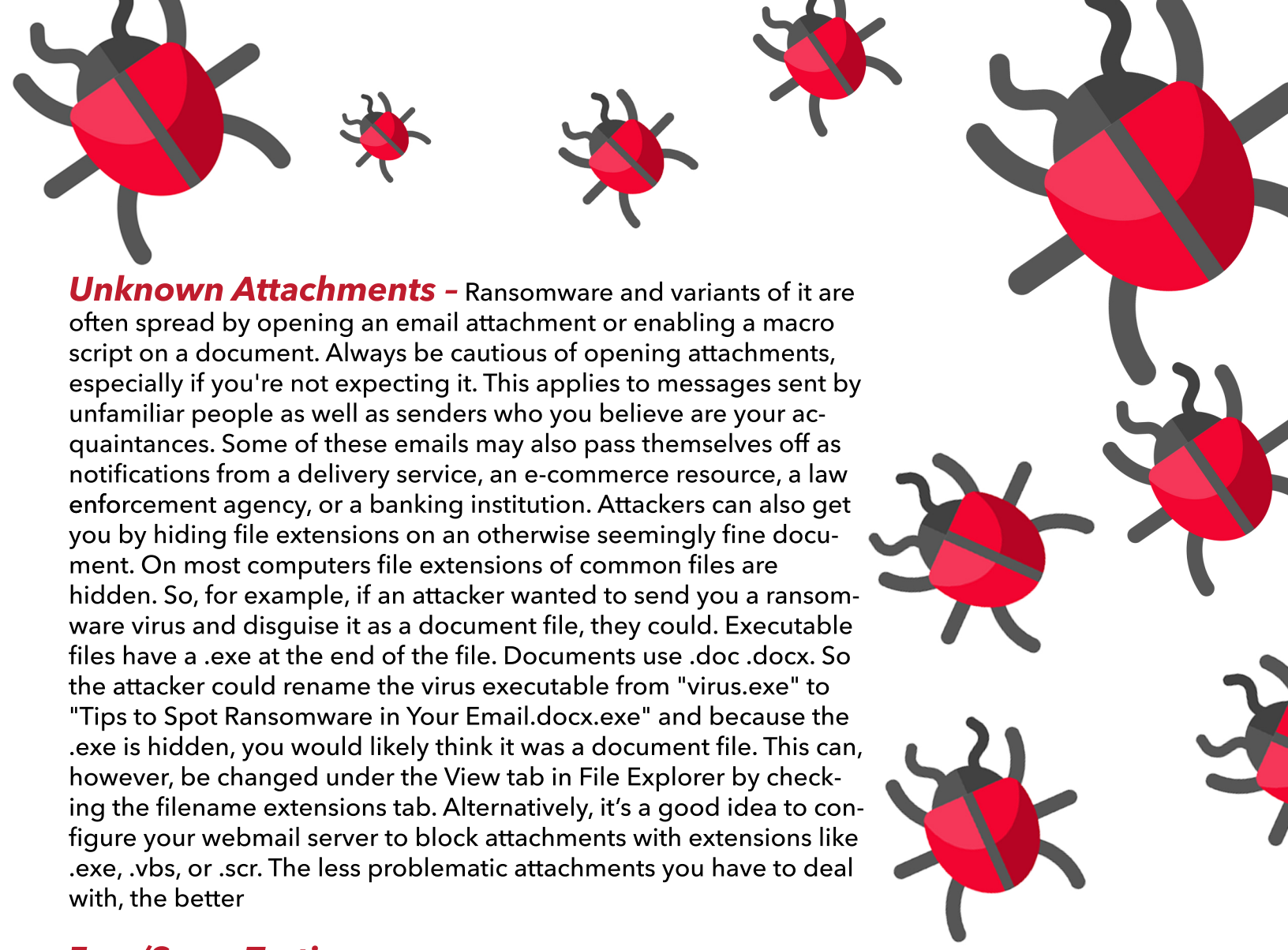
Bad grammar/spelling (corrected) – Most people take a sense of pride in their work. Bad grammar, typos, and spelling are a dead giveaway that there is something fishy happening (or "phishy" in the case of phishing scams).

It's an uncharacteristic request from somebody you know.

If you've ever received an email from someone you trust and/or know (e.g. your co-workers, your boss, the finance or legal department, etc.), but the language they're using now is different from normal somehow (either it's too formal or informal, or the email signature isn't the normal one used), then something weird might be going on. Their email has likely been spoofed or hacked, and the actual sender is trying to hack you as well.

Suspicious URL links –

It's very easy to hide or spoof a link. The display URL isn't necessarily the destination web page. And of course, you might click because some of these emails may also masquerade as notifications from an e-commerce resource (i.e. online retail store), a delivery service, a law enforcement agency, or a banking institution. Worse, emails with bad links can even be sent from your friends' or colleagues' email addresses. Cybercriminals can submit bad links to as many people as possible from your friends' or colleagues' email addresses by either spoofing the addresses without hacking their accounts (yes, this can be done) or by compromising their email accounts. So before you even click, hover over links to see if they direct you where you expect them to. Looks legitimate? Double check to look for individual characters or minor discrepancies. When in doubt, don't click. Delete!



Unknown Attachments – Ransomware and variants of it are often spread by opening an email attachment or enabling a macro script on a document. Always be cautious of opening attachments, especially if you're not expecting it. This applies to messages sent by unfamiliar people as well as senders who you believe are your acquaintances. Some of these emails may also pass themselves off as notifications from a delivery service, an e-commerce resource, a law enforcement agency, or a banking institution. Attackers can also get you by hiding file extensions on an otherwise seemingly fine document. On most computers file extensions of common files are hidden. So, for example, if an attacker wanted to send you a ransomware virus and disguise it as a document file, they could. Executable files have a .exe at the end of the file. Documents use .doc .docx. So the attacker could rename the virus executable from "virus.exe" to "Tips to Spot Ransomware in Your Email.docx.exe" and because the .exe is hidden, you would likely think it was a document file. This can, however, be changed under the View tab in File Explorer by checking the filename extensions tab. Alternatively, it's a good idea to configure your webmail server to block attachments with extensions like .exe, .vbs, or .scr. The less problematic attachments you have to deal with, the better

Fear/Scare Tactics – A common method used by cybercriminals is to use a line such as "your account has been breached!" in the subject line and email content. This alarms the email recipient and creates a sense of urgency and vulnerability, making them want to open the email and click quickly to address the issue. If you receive an email like this, take a moment before even opening it. If the claims in the email were true, would the sender really tell you in this way? Always check through a different means of communication (such as typing the usual URL into another tab or browser window and manually logging in to your account to see if your account information or messages match the information in the email, or calling the company).

Emails for Sweepstakes/Contests That You Never Entered – Ever receive emails for a sweepstakes/contest you didn't even enter? (This is even stranger if you're receiving these emails in your email inbox at work, as most people sign up for sweepstakes and contests with a personal email.) This sounds so obvious, but cybercriminals wouldn't send these types of emails if no one was clicking on their links.

If you don't remember or have a record of entering that sweepstakes/contest and it seems too good to be true, it's a scam. Do NOT click on the link to the prize page.

BONUS: Whenever you know you've received a spoof email masquerading as a major company (like Amazon, eBay, PayPal, or a banking institution), keep in mind that some of those companies have email addresses that you can forward the spoof email to before you delete it. They want to address this issue because these ransomware emails damage their brand and their bottom line, as their clients/customers might begin avoiding their emails altogether. Find out if the company being spoofed in your email has an email address set up for spam emails, and then forward whatever fake emails you receive

Even if the company doesn't have a set email for this, you can always forward the emails to their customer service email address before you delete them entirely. (Of course, if you haven't opened the email and don't feel comfortable doing so, then don't. Just delete. Better safe than sorry.)
Following these tips when reading through your emails can help you avoid ransomware (and other malware) attacks at work or at home, and will save you time, money and frustration in the long run

MAXtech