Stay Safe Online With Our Ransomware Cheat Sheet

PREDATORS ARE LURKING IN THE CONCRETE JUNGLE

COM · PRO
Managed Business Solutions

Ensure Your Email Attachments Don't Attach Something Dangerous

1. Never open attachments you're not expecting, EVEN IF IT LOOKS LIKE IT CAME FROM SOMEONE YOU KNOW. Email addresses can be easily faked, aka "spoofed".

2. Even if the attachment seems legit and from an email you know, DO NOT reply to the original email. It may just end up with the perpetrator, who will continue to play you like a fiddle. Instead, reply in a separate email or by phone call.

3. Banks and financial institutions rarely send attachments via email unless previously arranged. Even then, if you receive an email from a bank, there is a high probability that it is bogus. One easy way to spot an impostor is to check if the email is sent TO a generic user or FROM a generic user. If so, then beware!

4. Be extremely careful about opening PDF's. They may look innocent, but in many cases, they are NOT a PDF, but a script that installs the ransomware virus.

5. If you happen to open an attachment (for example, a PDF), most times there will be a link in the PDF for you to click. The text that is linked can be deceiving and can lead to a cyber trap. But hover your mouse over the link for a moment and it will tell you where the link actually goes.

Be Wary of Web Links

1. Email links can be as dangerous as attachments. Be careful! In a cleverly crafted email, links can appear legit, but actually lead you to a compromised website that can infect your devices with a ransomware script that runs in the background.

2. Some emails with bogus links will threaten you with a loss of service or a locked-out account, all in an attempt to frighten or intimidate you into action. Do not respond to these emails or click on their links! Contact your service provider instead if you have any concerns about your services.

3. A great way to spot a fraudulent link: Use the same “mouse hover” technique. Hover your mouse over the link and it will show you where the link actually goes, which could very well be a different location than it appears to be.

Use 'Password Smart' Strategies

1. Don't use weak passwords. Weak user passwords are commonly exploited by hackers to gain access to outward-facing corporate resources like web servers and/or remote access to terminal servers.

2. Ditch the simple passwords. They may be easy to remember, but they're also easy for others to guess. Simple passwords include your username, your birthday, or simple words like the word "password", "qwerty" or "12345".

3. Use password 'Best Practices'. Create passwords that include a minimum of 8-12 characters with one numeral, one capital, and one 'special character' (like a # or % or $).

4. Want even better password protection? Use a sentence instead (which is surprisingly easy to remember). Something like: "My all-time favourite movie is It's a *Wonderful Life*".

5. Add a few misspelled words to your password sentence. With a couple numerals, caps, and special characters, you have one hard-to-guess password. Example: "My all-tim favourite mo0vie is *It's a Wonderful Life*". Once you repeat it to yourself a few times it will become second-nature.

6. Don't reuse passwords! Passwords should be unique to each site. Get a password keeper app – they are free and easy to use.

7. Watch what you share on social media, especially if your passwords are based on people, places, or pets about which you post. A good cybercriminal will do his homework and will look for common themes on your social pages.

With a few of these essential do's and don'ts, you will be that much safer from ransomware and the cyberthieves behind them. Remember, also, to use your intuition. If an email or link seems a little suspect, it's best to not click on it or reply. Use your cyber sense and these tips and you'll be able to use your device securely and confidently.

COM · PRO
Managed Business Solutions

CONTACT US

Head Office:
18515 53rd Avenue
Suite 110
Surrey, BC, V3S 7A4

TF: 1-866-266-7761
T: 604-574-8623
F: 604-574-8634

Vancouver Office:
1108 W 8th Avenue
Vancouver, BC, V6H 3Z5

T: 604-664-8901
F: 604-900-3377