Cyber Security Best Practices Reminder

happier IT®

Cyber Security: Best Practices Reminder

As the COVID-19 outbreak continues, scammers and hackers are taking advantage of the fear and confusion surrounding the current circumstances by posing as reputable news sources, or offering information. These malicious actors are using the stress and the urgency of the current situation to misappropriate personal information, download malware, and attempt to scam money from consumers. These criminals are the online version of “looters” seeking to take advantage of a societal crisis.

Many businesses have instructed their employees to work from home wherever possible. Being "home alone", dealing with the stress of the overall situation, and receiving a higher number of texts, calls, and emails, puts individuals at a higher risk of accidentally falling victim to a scam.

Cyber Security Best Practices

Avoid clicking on links

Hovering the cursor over any links can help determine if it has been spoofed, but many malicious websites can look identical to the legitimate site. Consider whether an entity should be sending you a link in the first place, and if there is a way to simply navigate there through a search engine instead.

Be wary of email attachments

Unsolicited emails requesting that the user download and open an attachment is often a vector for malware.

Cyber Security:
Best Practices Reminder - continued

Be suspicious of unsolicited calls, texts, and emails

If you are unsure if a request is legitimate, verify before responding. Check previous invoices and communications for contact information, instead of trusting what was provided by the potential scammer.

Be cautious of "urgent"

A common approach for scammers is to pretend that something is urgent, and in a pandemic this is even more important to notice. Reputable institutions will not pressure you into making an immediate purchase or providing personal information instantly.

Use only trusted sources for information

Only get information from trusted government, healthcare, financial, and other verified information.

Do not reveal information about your organization

Scammers may call requesting information about your organization's structure, networks, and contacts. Do not reveal that information unless you have verified that the recipient has the authority to know it.

Do not reveal personal or financial information

Do not respond to emails requesting this information, and do not provide it over the phone if asked. Don't be afraid to say no or to hang up right away.