INTEGRITY MARKETING GROUP

WORKING FROM HOME SECURELY

Since so many of us are working remotely now, here's how to keep your data and equipment safe from home.

DON'T GET HOOKED BY PHISHING SCAMS

They're everywhere — emails or phone calls that seem legitimate but are meant to shock or lull you into reacting without thinking. And when you're working on your own, you need to be extra careful.

AVOID FAKE NEWS MESSAGES & MALICIOUS WEBSITES

These scams use fake stories or newsworthy events — like the coronavirus pandemic — to get you to click on a pop-up, link or social ad. Then, you're potentially exposed to malware and other threats.

SET STRONG, UNIQUE PASSWORDS

It seems obvious, but strong passwords can be the key to protecting your organization's most sensitive data. Ensure passwords you use for critical sites are unique and strong. It is recommended that you use at least eight characters, uppercase and lowercase letters mixed with numbers and at least one special character.

DON'T JUST RELY ON A PASSWORD ALONE

If it's an option, always use multi-factor authentication. This allows you to verify your username and password with a code that's sent to your phone or other mobile device.

GET WISE TO "CREDENTIAL PHISHING"

Like most phishing attacks, these scammers try to get you to give them your username and password — typically via a fake login page for a reputable-looking website. Avoid clicking on a link to update your account details. And bookmark the important sites you visit.

ALWAYS KEEP SOFTWARE UPDATED

Scammers constantly exploit security holes in outdated operating systems, plug-ins and other software. Keep your anti-virus software up to date and make sure you apply security patches when they're released.

MAKE SURE YOUR HOME WIFI NETWORK IS SECURE

Try these two essential tips: 1. Change your default router password from the one it came with ("admin" or "password," etc.) to your own unique one, and 2. Set a strong password for your Wi-Fi network via the WPA2 security settings.

KEEP YOUR WORK COMPUTER PRIVATE

Make sure you have a separate, private location to do your work, and ensure no one — including family members — can access your work computer. Also, make sure sensitive printed documents are locked away or shredded before discarding them.

USE A VIRTUAL PRIVATE NETWORK (VPN)

Using this secure network keeps your corporate network and internet browsing safe from criminals who want to intercept your data. Your IT security team can help you set one up.

FOLLOW ALL CORPORATE SECURITY POLICIES

That means finding and reading them in the first place. Then, make sure you follow all of them — and get the help you need to comply.

Remember, when you're working from home, you're the company's strongest defense. If you have any questions, or suspect any questionable activity, contact your IT security team immediately.