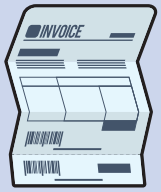
TOP 10 TIPS: TELEWORKING SECURELY

Due to our rapid shift to working remotely, many of us are now accessing corporate resources from **home environments that are far less secure than our office**. At the same time, scammers are actively exploiting heightened fears by launching countless coronavirus-themed campaigns. In fact, Barracuda Networks saw a **600% increase in phishing scams since February**. To help protect your critical data, our top 10 security recommendations are below.

1 DON'T CLICK LINKS OR ATTACHMENTS YOU WEREN'T EXPECTING (EMAIL OR TEXT)

It's very easy for scammers to impersonate legitimate sources.



2 CALL TO VERIFY REQUESTS FOR PERSONAL OR FINANCIAL INFORMATION

The more "urgent" the request the more likely it is a scam.

3 BE SUSPICIOUS OF MESSAGES WITH POOR SPELLING AND GRAMMAR

This is on purpose to weed out more savvy recipients quickly.

4 GET PANDEMIC UPDATES DIRECTLY FROM OFFICIAL SOURCES (WHO, CDC)

Everything you need to know is free and publicly accessible.

5 PROTECT HOME COMPUTERS WITH CENTRALIZED PATCHING AND ANTI-VIRUS

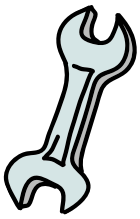
If you don't have company-owned equipment, this is second best.

6 CHANGE YOUR DEFAULT HOME ROUTER SETTINGS AND CONSIDER A VPN

For a VPN package, we recommend Perimeter 81 to our clients.

7 KEEP SOFTWARE APPLICATIONS UPDATED (DAILY IF USED HEAVILY)

Increased use uncovers more bugs, which leads to more patches.



8 USE STRONG PASSWORDS AND CONSIDER USING A PASSWORD MANAGER

We've found Keeper by Keeper Security best for corporate use.

9 ENFORCE MULTI-FACTOR AUTHENTICATION EVERYWHERE YOU CAN

This protects your accounts even if your username and password are stolen.

10 TURN OFF YOUR MACHINE THE MOMENT YOU SUSPECT AN INFECTION

And quickly follow that response by calling your IT support team.