BRAINSTORM

Scam Wise

REMOTE SECURITY DOS AND DON'TS

As remote work becomes the new norm, scammers are busier than ever. Here's what you need to know to keep your organization safe from the latest cyber security attacks.

AUTHENTICATION

40% of remote employees admit to transferring files between work and personal computers.[1]

DON'T use personal devices for work without appropriate security protocols in place.

DO follow security policies for company equipment and BYOD, paying special attention to multi-factor authentication and best practices for file sharing.

ATTACHMENTS

More than 48% of malicious email attachments are Office files and other common file types.

DON'T assume any email attachment is safe. Period.

DO ignore attachments unless they come from a trusted source. And when you collaborate, share your own attachments in Teams, SharePoint, or via OneDrive.

PHISHING

90% of data breaches come from phishing, with 1.5 M new phishing sites created every month.[3]

DON'T mindlessly click links or open attachments.

DO look for unknown senders, internal links, urgent requests for personal information, and offers that seem too good to be true. Check validity through Internet searches and report suspicious activity.

MALWARE

Email is responsible for 92% of malware attacks. Websites and apps take second place at 6%.[4]

DON'T fall for email trickery or put off critical system updates.

DO update your system, browsers, and plug-ins regularly. Additionally, log out of websites after browsing, back up important data, and remove unused or old software.

RANSOMWARE

Over 81% of ransomware attacks occur at enterprises, with email as the main distribution method.[5]

DON'T pay the ransom, no matter how desperate you feel.

DO create secure backups so you can always access critical files. If attacked, alert IT immediately.

IT SCAMS

Tech support scammers have convinced 1 in 5 consumers to continue with a fraudulent interaction.[6]

DON'T respond to unsolicited tech advice, even if the company looks reputable.

DO follow-up on legitimate websites where you can chat with an authorized tech support representative. Be suspicious of unsolicited phone calls, pop-up windows, or website redirects.

AWARENESS

70% of employees in the U.S. lack a basic understanding of security best practices.[7]

DON'T assume that employees don't have a role to play in improving your organization's security.

DO teach your employees to be savvy about cyber security issues. Use a platform like BrainStorm QuickHelp™ to automate your communications, poll your users, and build security skills.

BRAINSTORM

Want to change the way your users think about security?
Talk to a BrainStorm change expert.

Get Started

BrainStorm transforms organizations by using technology to empower people and activate change.

1. Ivanti | Remote work cyber security 2. CSO Online | 8 mobile security threats 3. Retruster | 2019 phishing and email fraud statistics 4. UMD Research | Malware data 5. Symantec | 2019 Internet security threat report 6. Microsoft | 2018 scam research 7. Hashed Out | 2019 cyber security statistics