Security

7 Risky Security Practices: Are Your Employees Doing Any of These?

LEAPFROG®
Extraordinary IT Services

Could your employees' bad habits be putting your company at risk? Your employees don't usually intend to be a weak link, but chances are they don't fully understand what they're supposed to do and why.

Great policies help employees develop great habits! Great policies are short, clear, specific and easy to follow. Too complicated or strict? They'll be ignored. Too vague or loose and, well, they'll be ignored.

Do any of these people work for you? Help them out! Here's what to do:

1. Password Patty

If anyone on your team writes passwords on sticky notes or doesn't bother logging out of their computers when they walk away, your company's data can be at risk. Not everyone in your office has the same security clearance and not everyone walking around your work environment is an employee.

WHAT TO DO: Tell employees exactly how you want them to handle passwords and logon/logout.

2. Social Sam

Updating social media sites with the latest tidbit can seem harmless enough. But in the heat of the moment it's easy to overshare. A juicy comment about a project, product, client, strategy, co-worker or in-office drama may come back to bite you. Hard. And as you know, once it's out there…

WHAT TO DO: Make a clear Do's and Don'ts List for social media sharing.

3. Texting Tyrone

Who on your team has an unlimited SMS plan? Probably everyone. Texting is often overlooked when it comes to company security — by policy-writing leadership and text-happy employees alike! Sending links, images and quick thoughts by text is handy but may fall outside of what your IT department can control or access.

WHAT TO DO: Don't forget to include texting guidelines in your policy.

4. Spacey Stacey

It can be embarrassing for someone to report a lost smartphone, especially if it's happened before. Or someone can feel foolish if they suspect information was accessed on any of their devices when they weren't paying attention. If the person has a reputation for carelessness, it can be even harder to confess another mistake.

WHAT TO DO: Make it easy for employees to come clean.

5. Gullible Grace

Occasionally phishing emails make it to inboxes even if you have the latest, greatest anti-malware and firewalls. There are just too many emails bombarding the email ecosystem. So whether it's a trusting nature, curiosity or mindless clicking, some people just don't practice safe emailing.

WHAT TO DO: Clarify which emails can be opened on devices used for work (and get a good IT services partner).

6. Resentful Rudy

Sometimes it's the little things. If you're not splitting the bill with your

employees for their personal smartphones when they use those phones for work (or picking up the tab entirely), you're making it easier for them to rationalize risky behavior.

WHAT TO DO: Put your money where your mouth is in your BYOD policy.

7. Efficient Evanna

Sometimes the fastest way to do something is exactly the opposite of how you want your employees to do it. Dropbox, thumb drives, emailing attachments with a gmail account — easy! Adhering to Intellectual Property (IP) policies that are too complicated or cumbersome — tedious.

WHAT TO DO: Choose systems that are safe for you and convenient for your employees.