Employee Exit Checklist for IT Security

Xlingshot

xlingshot.com

EMPLOYEE EXIT CHECKLIST

Did you know that 89% of employees still have a valid login and password to at least one business application after termination? This list will help protect you and your business after moving on from an ex-employee.

TAKE BACK ACCESS TO EMAIL

The employee no longer works for the organization. Therefore, you don't want them using your company email after termination.

DISABLE ALL INTERNAL USER ACCOUNTS CONNECTED TO THE EMPLOYEE

Any accounts the employee uses and has access to needs to be disabled prior to termination to avoid any potential security issues.

SET UP AUTO EMAIL FORWARDING

To make sure none of the emails go unread, be sure to setup auto forwarding to a current member of your team. Set up an auto responder for at least 30 days and introduce your clients to their new point of contact.

CHANGE COMPANY CREDIT CARD PINS

Did your former employee use a company card? Be sure to change their PIN.

TERMINATE VPN AND REMOTE-DESKTOP ACCESS

This one seems obvious, but can easily be overlooked. Today's VPN configurations tend to be complex, making it easy for the former employee to gain network access.

UPDATE COMPANY WIDE PASSWORDS

The exiting employee may have access to company wide passwords. Change passwords to ensure current employees of your company are the only ones accessing the information.

RECOVER PHYSICAL PROPERTY

If not done during termination, recover company property from the terminated employee such as laptop, smart phone, security key to your building, home printer, software, etc.

INFORM YOUR IT PARTNER

Informing your IT partner is one of the most important items on this list. They can help guide you through the off boarding process and apply "checks and balances" to reduce any threats.