What's New

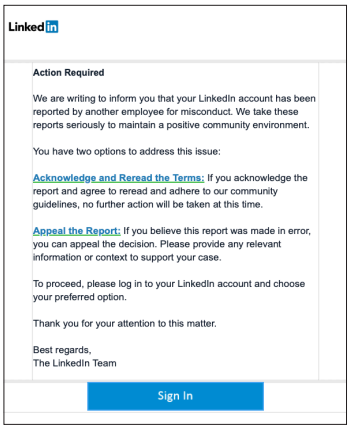
Here's a fresh look at the latest training content.

August 2024

Real World Threat Emails

These emails are based on emails flagged by Barracuda security and other real-world samples. Search for them by name in the SAT tool.

LinkedIn Account Reported



LinkedIn

Action Required

We are writing to inform you that your LinkedIn account has been reported by another employee for misconduct. We take these reports seriously to maintain a positive community environment.

You have two options to address this issue:

Acknowledge and Reread the Terms: If you acknowledge the report and agree to reread and adhere to our community guidelines, no further action will be taken at this time.

Appeal the Report: If you believe this report was made in error, you can appeal the decision. Please provide any relevant information or context to support your case.

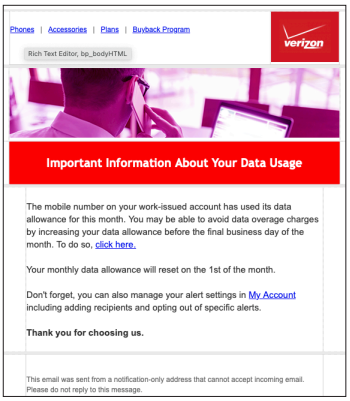
To proceed, please log in to your LinkedIn account and choose your preferred option.

Thank you for your attention to this matter.

Best regards,
The LinkedIn Team

Sign In

Verizon Data Overage



Phones | Accessories | Plans | Buyback Program

Rich Text Editor, bp_bodyHTML

Important Information About Your Data Usage

The mobile number on your work-issued account has used its data allowance for this month. You may be able to avoid data overage charges by increasing your data allowance before the final business day of the month. To do so, click here.

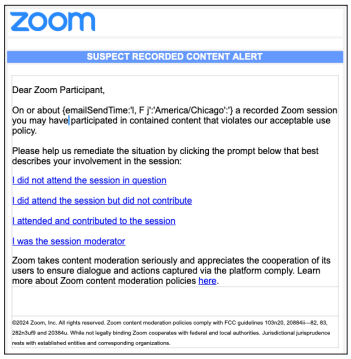
Your monthly data allowance will reset on the 1st of the month.

Don't forget, you can also manage your alert settings in My Account including adding recipients and opting out of specific alerts.

Thank you for choosing us.

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Zoom Suspect Content Alert



zoom

SUSPECT RECORDED CONTENT ALERT

Dear Zoom Participant,

On or about {emailSendTime:'l, F j,':'America/Chicago':'} a recorded Zoom session you may have participated in contained content that violates our acceptable use policy.

Please help us remediate the situation by clicking the prompt below that best describes your involvement in the session:

I did not attend the session in question

I did attend the session but did not contribute

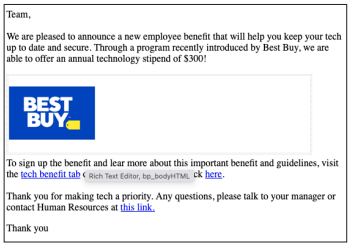
I attended and contributed to the session

I was the session moderator

Zoom takes content moderation seriously and appreciates the cooperation of its users to ensure dialogue and actions captured via the platform comply. Learn more about Zoom content moderation policies here.

©2024 Zoom, Inc. All rights reserved. Zoom content moderation policies comply with FCC guidelines 103n20, 208841—82, 83, 282n3uff9 and 203844u. While not legally binding Zoom cooperates with federal and local authorities. Jurisdictional jurisprudence rests with established entities and corresponding organizations.

Tech Upgrade Stipend



Team,

We are pleased to announce a new employee benefit that will help you keep your tech up to date and secure. Through a program recently introduced by Best Buy, we are able to offer an annual technology stipend of $300!

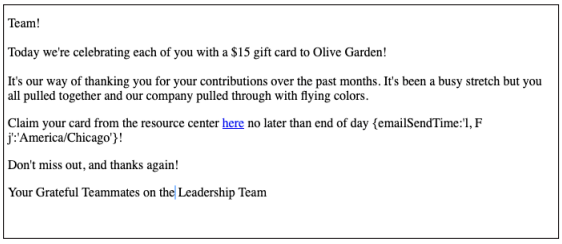
BEST BUY

To sign up the benefit and lear more about this important benefit and guidelines, visit the tech benefit tab (Rich Text Editor, bp_bodyHTML ck here.

Thank you for making tech a priority. Any questions, please talk to your manager or contact Human Resources at this link.

Thank you

Employee Appreciate Day



Team!

Today we're celebrating each of you with a $15 gift card to Olive Garden!

It's our way of thanking you for your contributions over the past months. It's been a busy stretch but you all pulled together and our company pulled through with flying colors.

Claim your card from the resource center here no later than end of day {emailSendTime:'l, F j':'America/Chicago'}!

Don't miss out, and thanks again!

Your Grateful Teammates on the Leadership Team

More on next page.

A digital newsletter for Barracuda Security Awareness Training. © 2024 Barracuda Networks Inc. All rights reserved.

August 2024

Lifestyle Bundle: Gadget Security

A guide to training that spotlights information security risks of wifi-connected devices. Available in the August 2024 Click Thinking bundle.

Barracuda

Lifestyle Bundle

Lifestyle Bundle: Gadget Security

Training for everyday living you can implement with ease.

Data Security Risks of Using Internet-Connected Devices and QR Codes

The integration of internet-connected devices and QR codes into everyday operations introduces several data security risks.

Internet-connected devices, often part of the Internet of Things (IoT), are susceptible to various threats due to their constant connectivity and often limited security measures. These devices can be targeted for unauthorized access, data breaches, and malware infections.

Weak passwords, unpatched vulnerabilities, and lack of encryption are common issues that can lead to compromised networks and data theft. Once an attacker gains access to a device, they can exploit it to infiltrate other parts of the network, leading to broader security breaches.

QR codes, though convenient for quick information access, also present significant security risks. Malicious QR codes can redirect users to phishing sites, prompting them to enter sensitive information like login credentials or financial details.

These codes can also trigger unintended actions on a user's device, such as downloading malware. The ease with which QR codes can be created and distributed makes it challenging to ensure their authenticity, increasing the likelihood of encountering a malicious code.

To mitigate these risks, organizations should implement robust security protocols, such as regularly updating device software, employing strong passwords, and educating users about the potential dangers of scanning unknown QR codes. By enhancing security measures and promoting awareness, the risks associated with internet-connected devices and QR codes can be significantly reduced.

Build Your Own Gadget Security Bundle

The modules below address a wide range of issues associated with wifi-connected gadgets and QR codes. Available in the Content Center now, just search them by number to make them part of your overall training curriculum.

Internet of Things A103A-4

A closer look at the risks of using internet-connected devices.

INTERNET OF THINGS

QR Code Safety A103A-24

Explores risks of using QR codes and how to spot and avoid them.

QR CODE SAFETY

Advanced QR Code Safety A103A-25

Reviews advanced risks and mitigation factors for QR code security.

ADVANCED QR CODE SAFETY

Barracuda Networks • Lifestyle Bundle • Lifestyle Bundle: Gadget Security
A digital newsletter for Barracuda Security Awareness Training. © 2024 Barracuda Networks Inc. All rights reserved.

Email Protection