Cybersecurity 101

KEEP THIS CARD ON YOUR DESK

1. Never click on suspicious hyperlinks in emails

Avoid clicking on hyperlinks, especially from unknown senders. **Hover your mouse** over links in emails to make sure they go to a legitimate website—check carefully for typos, such as "arnazon.com." Do not click on long hyperlinks sent to you without context.

2. Beware of unusual and unexpected emails

Exercise caution with emails not related to your job responsibilities, that were sent at **odd times**, and that seem oddly phrased or **out-of-character** for the sender. Watch out for unusual bad grammar and **spelling mistakes**.

3. Study the 'from' line

Beware of emails from outside your firm or from strangers. Make sure the **sender's name and domain are not misspelled** or otherwise suspicious.

4. Look out for cc'ed strangers

Do not trust an email that has cc'ed people you do not know or that was sent to a **random mix** of people at your firm.

5. Treat emails requesting fund transfers with suspicion

Do not open links or attachments under **threat of a negative consequence** or the promise of gaining something. All emails requesting fund transfers are suspect. Do not click on emails asking you to look at a **compromising picture** of yourself or someone you know.

6. Watch for weird subject lines

Watch out for emails that have **irrelevant subject lines** that do not match the email's content, as well as messages that reply to something you never sent or requested.

7. Do not click on suspicious attachments, especially PDFs

Do not click on attachments that are from unknown senders, are **unexpected**, or do not relate to the content of the email message.

8. Delete suspected phishing emails immediately

Do not click on any links in a suspected phishing email. Delete the email and **alert your IT team** or security administrator.

9. Never enter sensitive information into a pop-up window

Avoid clicking on pop-up windows or **block them** altogether.

10. Verify HTTPS in the address bar

When entering confidential information online, confirm that the address bar reads **"HTTPS."** The "S" confirms safety.

To learn more about how you can proactively protect yourself with the right technology and training, write to us at **hello@kraftkennedy.com.**

Kraft
Kennedy

IF YOU BELIEVE YOU HAVE BEEN COMPROMISED, CONTACT YOUR IT TEAM.

FOR PROACTIVE PROTECTION, CONTACT KRAFT KENNEDY: (800) 523-3081

OUR SECURITY EXPERTS ARE AVAILABLE 24/7 FOR OUR CLIENTS.

DOCUMENT MANAGEMENT & INFORMATION PROTECTION

PROJECT MANAGEMENT OFFICE AS A SERVICE

MESSAGING & UNIFIED COMMUNICATIONS

INFRASTRUCTURE & VIRTUALIZATION

ENTERPRISE ESCALATION SUPPORT

DESKTOP LIFECYCLE MANAGEMENT

MANAGED SERVICES & SUPPORT

SECURITY OPERATIONS CENTER

STAFF AUGMENTATION

CLOUD SERVICES

Kraft Kennedy

hello@kraftkennedy.com
kraftkennedy.com
(800) 523-3081